Descripción de Cisco AMP para los puntos finales API

Contenido

Introducción

Este documento describe sobre la protección avanzada Cisco de Malware (AMP) para los puntos finales. Cisco AMP para los puntos finales viene con una interfaz de programación de aplicaciones (API). Permite que usted tire de los datos de un AMP para el despliegue de los puntos finales, y los manipula, cuando sea necesario.

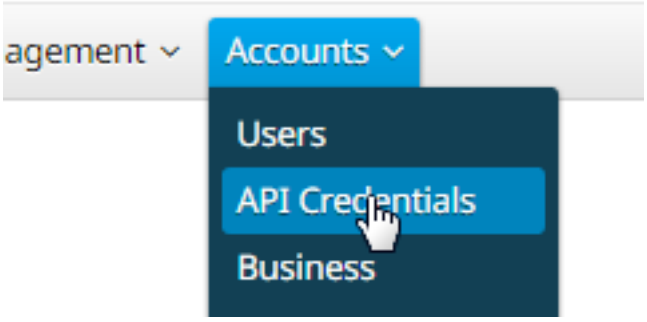
Este artículo demuestra algunas funcionalidades básicas del API. Los ejemplos en este artículo utilizan un punto final de Windows 7.

Contribuido por las cartas francas de Matthew, Nazmul Rajib, y los ingenieros de Cisco TAC.

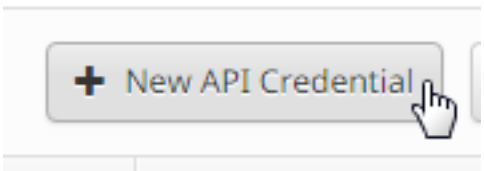
Genere y borre las credenciales API

Para utilizar el AMP para el punto final API, usted tiene que configurar los credenciales API. Siga los pasos dados para crear los credenciales a través de la consola AMP.

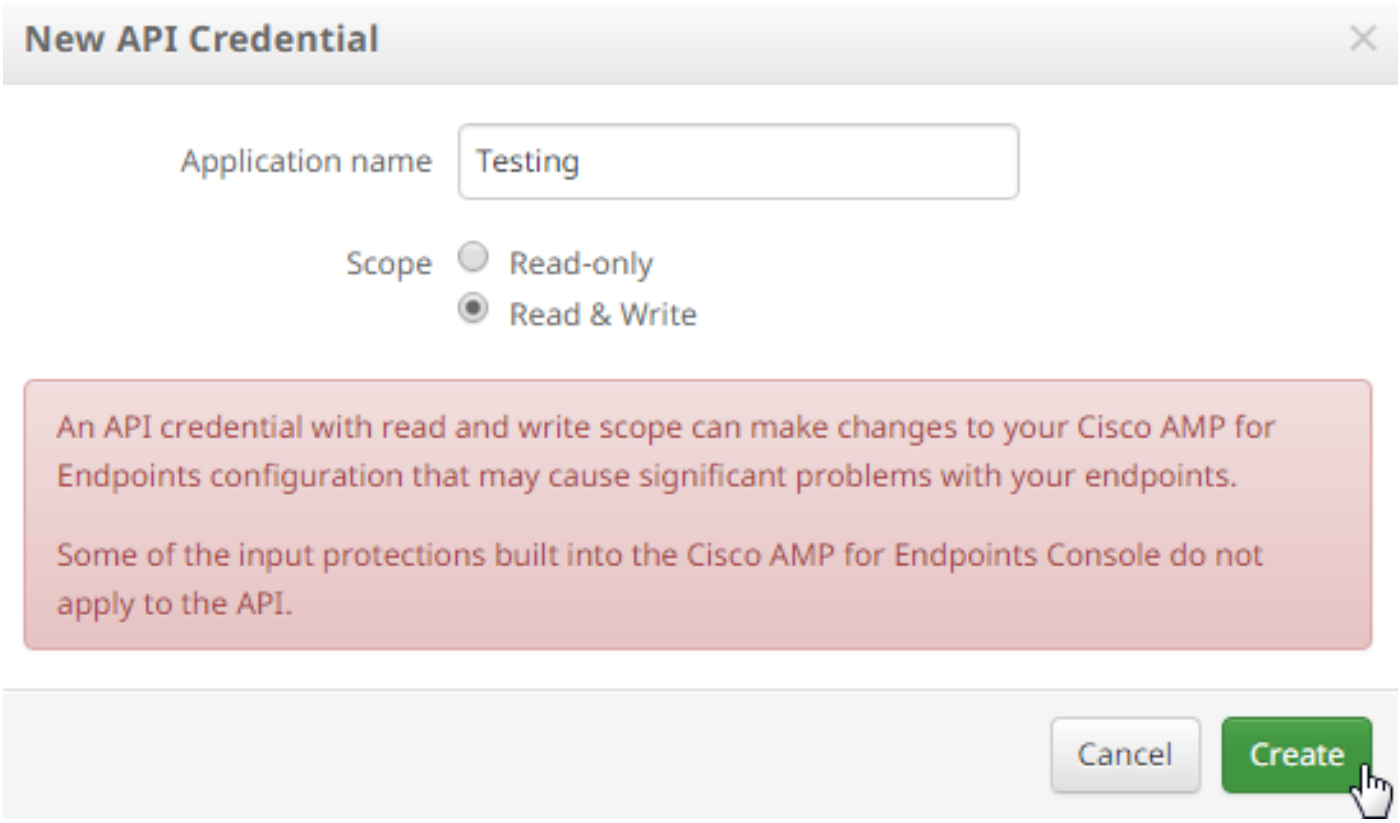
Paso 1: El registro en la consola, y navega a las **cuentas > a las credenciales API.**



Paso 2: Haga clic los **nuevos credenciales API** para crear un nuevo conjunto de las claves.

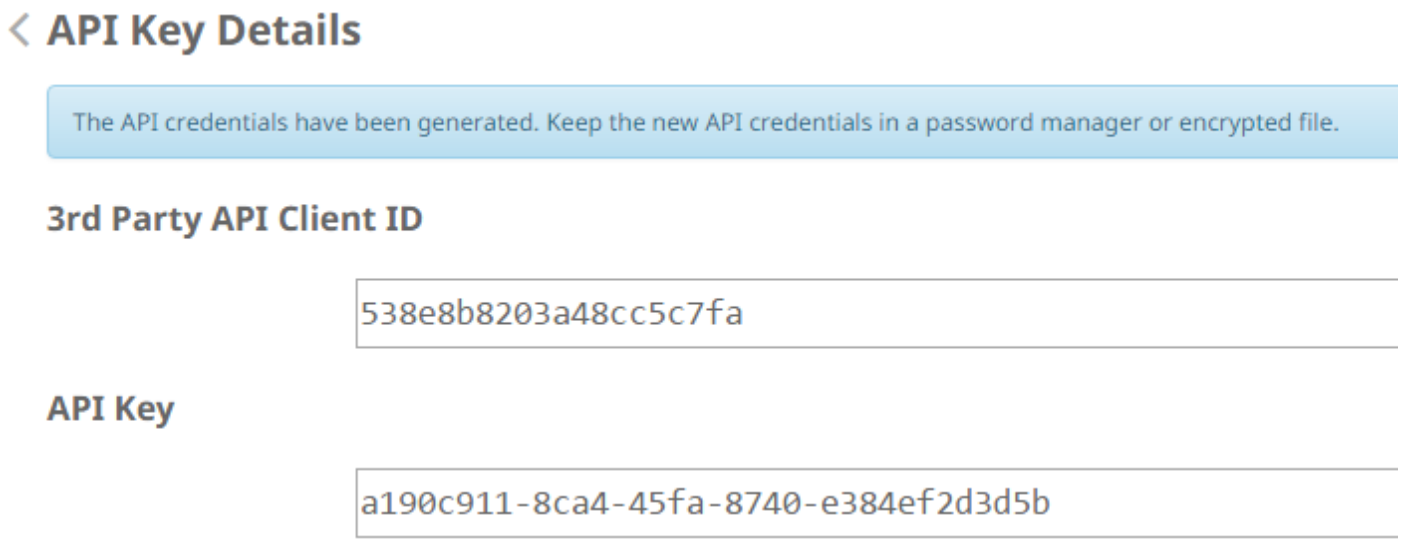


Paso 3: Proporcione un **nombre de la aplicación**. Seleccione el **alcance de** solo lectura o lea y escriba.



Note: Los credenciales API con leído y escriben el alcance pueden realizar los cambios a su Cisco AMP para la configuración de los puntos finales que pudo causar los problemas importantes con sus puntos finales. Algunas de las protecciones de la entrada incorporadas a Cisco AMP para la consola de los puntos finales no se aplican al API.

Paso 4: Haga clic el **botón Create**. **Los detalles de la clave API** aparecen. Salve esta información pues algo de él no estará disponible después de dejar la pantalla.

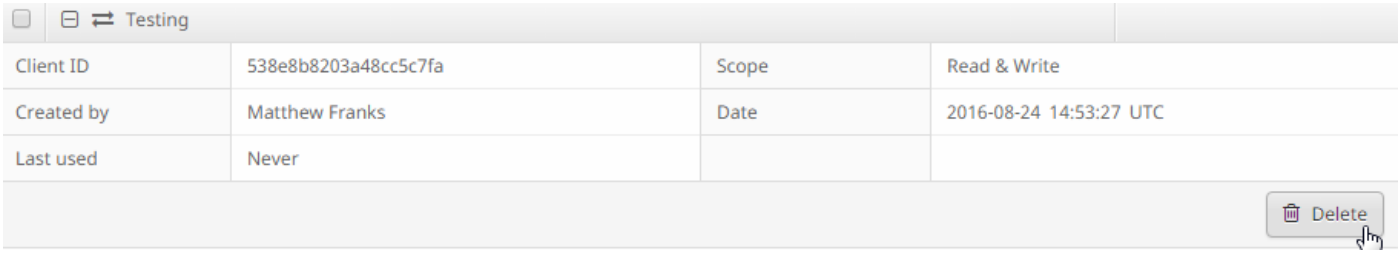


Note: Las credenciales API (ID de cliente API y clave API) permitirán que otros programas extraigan y modifiquen su Cisco AMP para los datos de los puntos finales. Es funcionalmente equivalente a un nombre de usuario y contraseña, y debe ser tratado como

tal.

Caution: Sus credenciales API se visualizan una vez solamente. Si usted pierde las credenciales, usted tiene que generar los nuevos.

Borre las credenciales API para una aplicación si usted sospecha que se han comprometido, y que crean un nuevo. Cuando usted borra los credenciales API, bloquean hacia fuera al cliente que utiliza los viejos, los ponen al día tan con las nuevas credenciales.



Versiones API y opciones actuales

Hay actualmente dos versiones del AMP para los puntos finales API - versión 0 y versión 1. La versión 1 tiene funciones adicionales contra la versión 0. La documentación para la versión 1 está aquí. Usted puede tirar de este witn de la información el uso de la versión 1.

- Computadoras
- Actividad de la Computadora
- Eventos
- Tipos de evento
- Listas de archivos
- Elementos de la lista de archivos
- Grupos
- Directivas
- Versiones

Haga clic en el comando relevant en el documento de ver los ejemplos de su uso.

El API ordena la ruptura y el ejemplo

Cada comando API contiene la información similar y puede esencialmente analizar a un comando del rizo y se puede parecer esto:

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

Cuando usted utiliza el comando del rizo con – opción `o`, permite que usted salve la salida a un archivo. En este caso el nombre del archivo es "`yourfilename.json`".

Tip: Más información sobre los archivos .json se puede encontrar aquí.

El siguiente paso en el comando del **rizo** es fijar el direccionamiento con sus credenciales antes @ del símbolo. Cuando usted las credenciales del generatie API, usted conoce el clientID y el

APIKey, así que esta sección del comando se asemejará al link dado abajo.

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

Agregue el número de la versión y qué usted quisiera hacer. Por este ejemplo, ejecute las opciones GET /v1/computers. El comando completo parece esto:

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

Después de que usted funcione con el comando, usted debe ver un **archivo computers.json** descargado al directorio donde usted inició el comando.

```
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
```

> **Note**: El rizo es accesible en línea y compilado para las porciones de Plataformas que incluye Windows (usted querrá generalmente utilizar Win32 – versión genérica).

Cuando usted abre el archivo usted verá todos los datos en una sola línea. Si usted quisiera ver esto en su formato apropiado, usted puede instalar a un navegador plug-in para formatarlo como JSON y para abrir el archivo en un navegador. Esto muestra que la información para sus ordenadores que usted puede utilizar sin embargo usted quisiera, por ejemplo:

connector_guid, nombre de host, active, links, connector_version, operating_system, internal_ips, external_ip, group_guid, network_addresses, guid de la directiva, y nombre de la directiva.


```
{
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"
}
```


Ahora que usted ha visto un ejemplo básico en la acción, usted puede utilizar el diverso comando options de tirar y de manipular de los datos en su entorno.

Información Relacionada

- Cisco AMP para la documentación de los puntos finales API

Soporte Técnico y Documentación - Cisco Systems