

Descripción de Cisco amperio para los puntos finales API

Contenido

[Información general](#)

[Generando y borrando las credenciales API](#)

[Versiones API y opciones actuales](#)

[Ruptura y ejemplo del comando API](#)

[Documentos Relacionados](#)

Información general

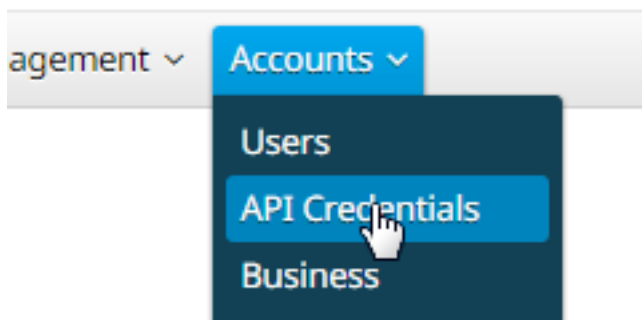
Cisco amperio para los puntos finales viene con un API. Permite que usted tire de los datos de un amperio para el despliegue de los puntos finales, y los manipula, cuando sea necesario.

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

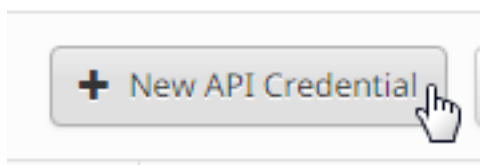
Generando y borrando las credenciales API

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

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



Paso 2: **Nuevos API credenciales** del teclado 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**.

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

Note: Los credenciales API con leído y escriben el alcance pueden realizar los cambios a su Cisco amperio para la configuración de los puntos finales que puede causar los problemas importantes con sus puntos finales. Algunas de las protecciones de la entrada incorporadas a Cisco amperio 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. Esté seguro de salvar esta información pues algo de él no estará disponible después de dejar esta pantalla.

< 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

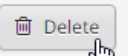
a190c911-8ca4-45fa-8740-e384ef2d3d5b

Note: Las credenciales API (ID de cliente API y clave API) permitirán que otros programas extraigan y modifiquen su Cisco amperio 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. Borrar los credenciales API bloquea hacia fuera al cliente que utiliza los viejos, así que se asegure ponerlos al día con las nuevas credenciales.

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



Versiones API y opciones actuales

Hay actualmente dos versiones del amperio para los puntos finales API - versión 0 y versión 1. La versión 1 que tiene funciones adicionales contra la versión 0. La documentación para la versión 1 está [aquí](#). Usted puede tirar de la siguiente información usando 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 la documentación de ver los ejemplos de su uso.

Ruptura y ejemplo del comando API

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

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

Usando el comando del rizo con `-o` la 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. De la información en las credenciales de generación sección API, conocemos el clientID y el APIKey, así que esta sección del comando se asemejaría:

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

Después, agregamos el número de la versión y qué quisiéramos hacer. Por este ejemplo ejecutaremos las opciones [GET /v1/computers](#). El comando completo parece abajo:

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

```
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 incluyendo 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.sourcefire.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.sourcefire.com/v1/computers/abcdef-1234-5678-9abc-def123456789",
        trajectory: "https://api.amp.sourcefire.com/v1/computers/abcdef-1234-5678-9abc-def123456789/trajectory",
        group: "https://api.amp.sourcefire.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.

Documentos Relacionados

- [Cisco amperio para la documentación de los puntos finales API](#)