Vista geral de Cisco AMP para os valores-limite API

Índice

Introdução

Este documento descreve sobre a proteção avançada Cisco do malware (AMP) para valores-limite. Cisco AMP para valores-limite vem com uma interface de programação de aplicativo (API). Permite que você puxe dados de um AMP para o desenvolvimento dos valores-limite, e manipula-os, quando necessário.

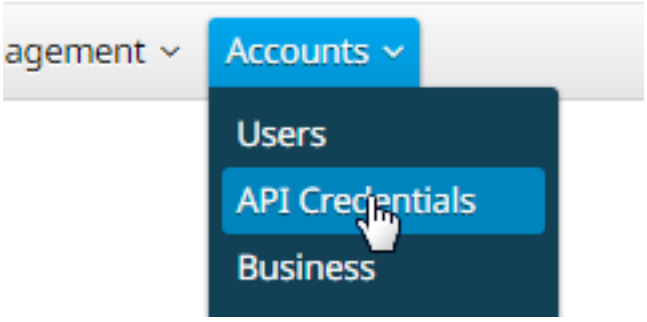
Este artigo demonstra algumas funcionalidades básicas do API. Os exemplos neste artigo usam um valor-limite de Windows 7.

Contribuído por franquias de Matthew, por Nazmul Rajib, e por engenheiros de TAC da Cisco.

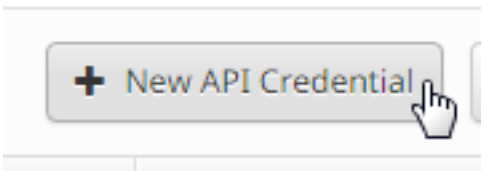
Gerencia e suprima de credenciais API

A fim usar o AMP para o valor-limite API, você tem que estabelecer umas credenciais API. Siga as etapas dadas para criar umas credenciais através do console AMP.

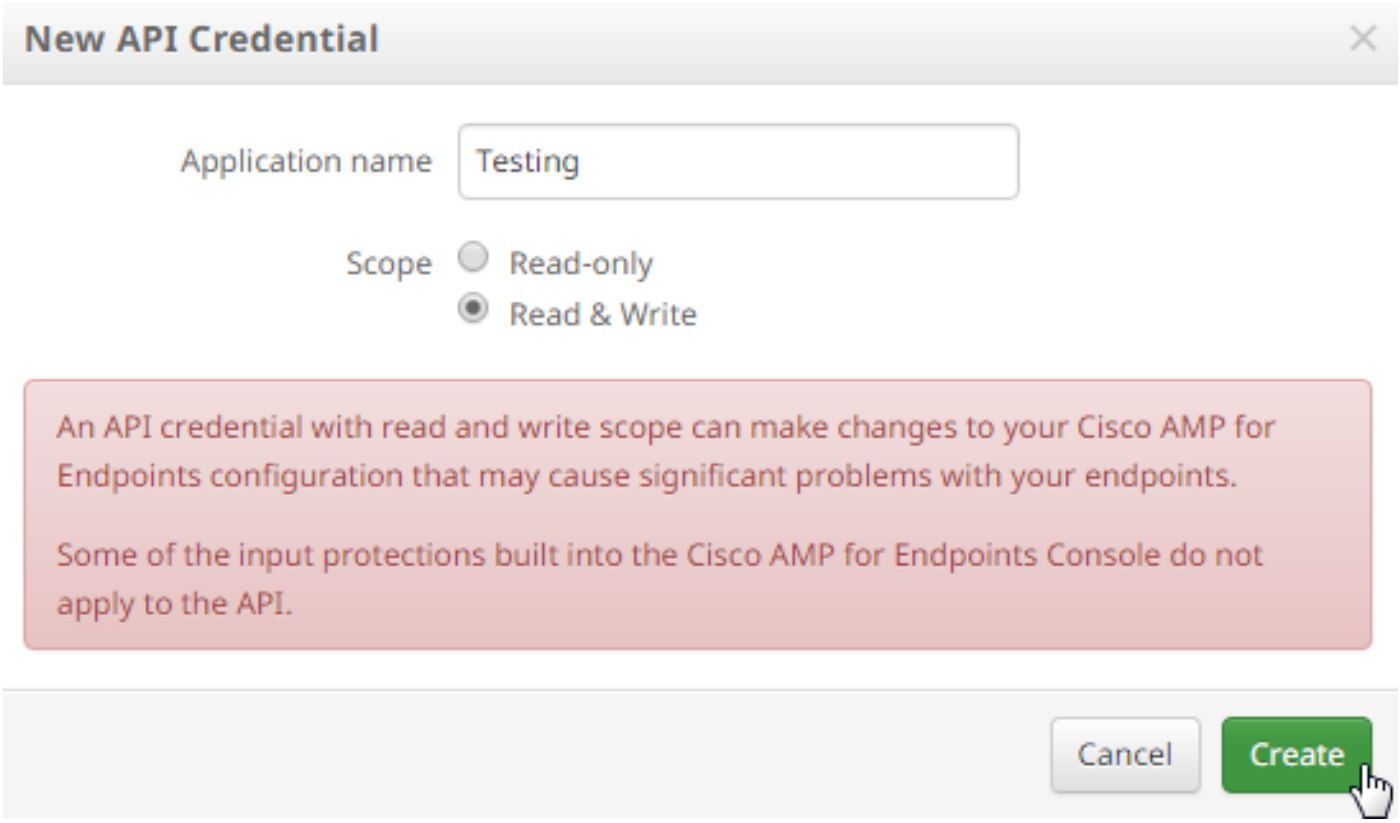
Passo 1: O log no console, e navega às **contas > às credenciais API.**



Passo 2: Clique **credenciais novas API** para criar um grupo novo de chaves.

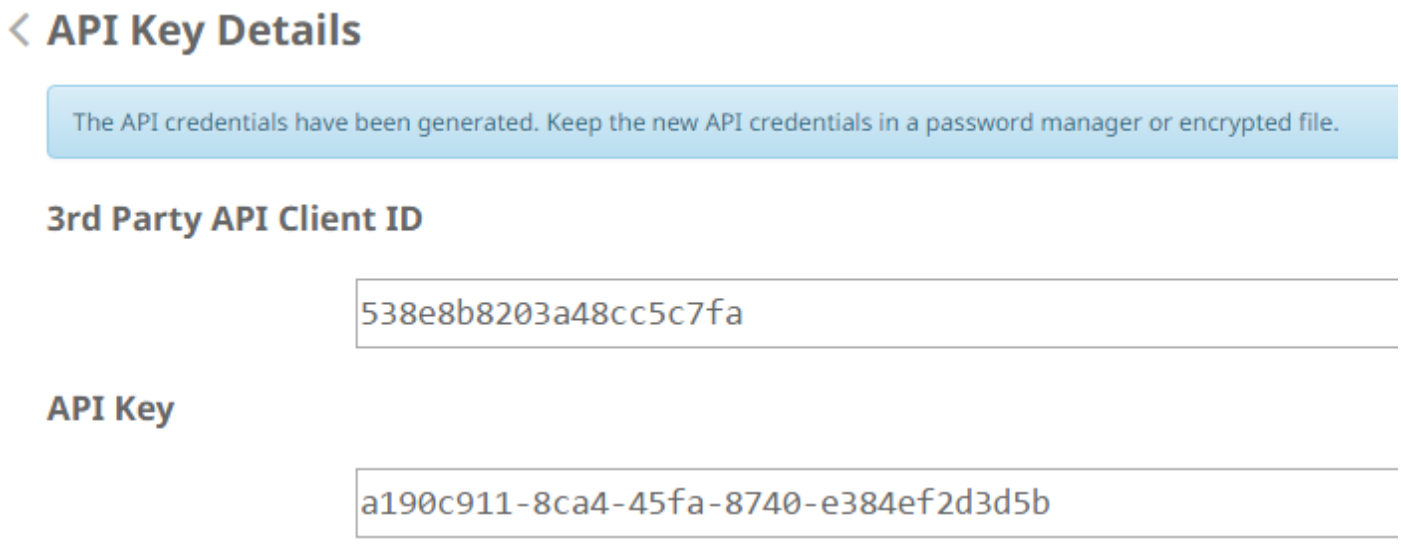


Passo 3: Forneça um **nome do aplicativo**. Selecione o **espaço de** leitura apenas ou leia-o & escreva-o.



Note: Umas credenciais API com lido e escrevem o espaço podem fazer mudanças a seu Cisco AMP para a configuração dos valores-limite que pôde causar problemas significativos com seus valores-limite. Algumas das proteções da entrada construídas em Cisco AMP para o console dos valores-limite não se aplicam ao API.

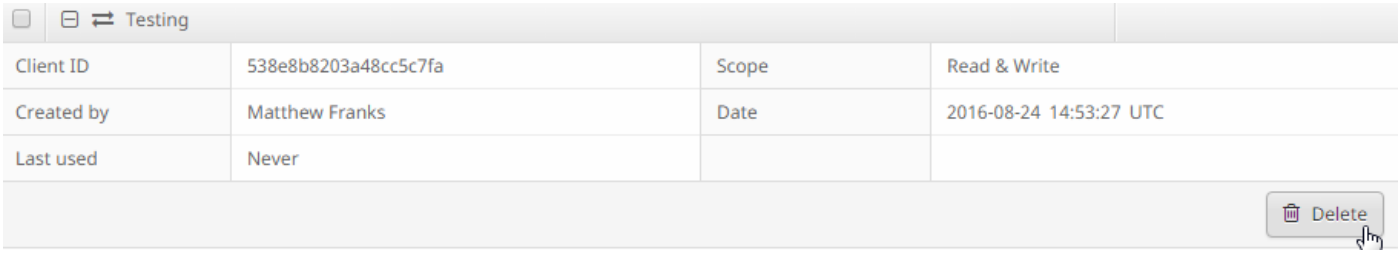
Passo 4: Clique o **botão Create**. **Os detalhes da chave API** aparecem. Salvar esta informação porque alguma dele não estará disponível após ter deixado a tela.



Note: As credenciais API (identificação de cliente API & chave API) permitirão que outros programas recuperem e alterem seu Cisco AMP para dados dos valores-limite. É funcionalmente equivalente a um nome de usuário e senha, e deve ser tratado como tal.

Caution: Suas credenciais API são indicadas uma vez somente. Se você perde as credenciais, você tem que gerar novos.

Suprima das credenciais API para um aplicativo se você suspeita que estiveram comprometidas, e criam um novo. Quando você suprime de umas credenciais API, travam para fora o cliente que usa velhos, atualizam-nos assim com as credenciais novas.



Versões API e opções atuais

Há atualmente duas versões do AMP para os valores-limite API - versão 0 e versão 1. A versão 1 tem a funcionalidade adicional contra a versão 0. A documentação para a versão 1 está aqui. Você pode puxar este witn da informação o uso da versão 1.

- Computadores
- Atividade do computador
- Eventos
- Tipos de evento
- Lista do arquivo
- Artigos da lista do arquivo
- Grupos
- Políticas
- Versões

Clique sobre o comando relevant no documento ver exemplos de seu uso.

O API comanda a divisão e o exemplo

Cada comando API contém a informação similar e pode essencialmente dividir a um comando da onda e pode ser olhado como este:

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

Quando você usa o comando da onda com – opção `o`, permite que você salvar a saída a um arquivo. Neste caso o nome de arquivo é “`yourfilename.json`”.

Tip: Mais informação em arquivos .json pode ser encontrada aqui.

A próxima etapa no comando da **onda** é ajustar o endereço com suas credenciais antes @ do símbolo. Quando você credenciais do generatie API, você conhece o clientID e o APIKey, assim que esta seção do comando assemelhar-se-á ao link dado abaixo.

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

Adicionar o número de versão e o que você gostaria de fazer. Para este exemplo, execute as opções GET /v1/computers. O comando cheio olha como este:

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

Depois que você executa o comando, você deve ver um **arquivo computers.json** transferido ao diretório onde você iniciou o 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**: A onda é acessível em linha e compilada para lotes das Plataformas que inclui Windows (geralmente você quererá usar Win32 – versão genérica).

Quando você abre o arquivo você verá todos os dados em uma linha única. Se você gostaria de ver este em seu formato apropriado, você pode instalar um navegador de encaixe para formatá-lo como JSON e para abrir o arquivo em um navegador. Isto mostra que a informação para seus computadores que você pode se usar contudo você gostaria, como:

connector_guid, hostname, active, links, connector_version, operating_system, internal_ips, external_ip, group_guid, network_addresses, guid da política, e nome da política.


```
{
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"
}
```


Agora que você viu um exemplo básico na ação, você pode usar o vário comando options puxar e manipular dados em seu ambiente.

Informações Relacionadas

- Cisco AMP para a documentação dos valores-limite API

Suporte Técnico e Documentação - Cisco Systems