

Vista geral de Cisco ampère para os valores-limite API

Índice

[Visão geral](#)

[Gerando e suprimindo de credenciais API](#)

[Versões API e opções atuais](#)

[Divisão e exemplo do comando API](#)

[Documentos relacionados](#)

Visão geral

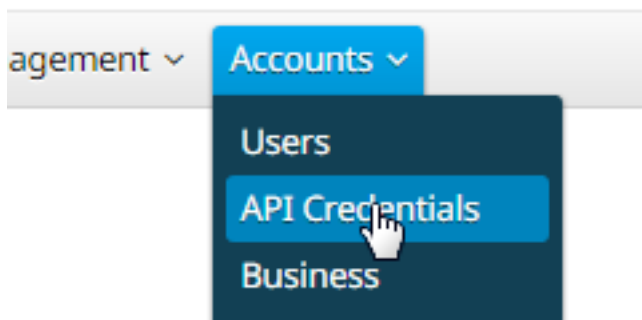
Cisco ampère para valores-limite vem com um API. Permite que você puxe dados de um ampère para o desenvolvimento dos valores-limite, e manipula-os, quando necessário.

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

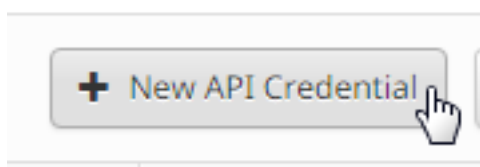
Gerando e suprimindo de credenciais API

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

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



Passo 2: **Credenciais novas** do clique **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**.

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

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

< 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

API Key

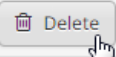
Note: As credenciais API (identificação de cliente API & chave API) permitirão que outros programas recuperem e alterem seu Cisco ampère para dados dos valores-limite. É funcionalmente equivalente a um nome de usuário e senha, e deve ser tratado como tal.

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 crie um novo. Suprimir de umas credenciais API trava para fora o cliente que usa velhos, assim que certifica-se actualizá-los com as credenciais novas.

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



Versões API e opções atuais

Há atualmente duas versões do ampère para os valores-limite API - versão 0 e versão 1. A versão 1 que tem a funcionalidade adicional contra a versão 0. A documentação para a versão 1 está [aqui](#). Você pode puxar a informação seguinte usando a 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 na documentação ver exemplos de seu uso.

Divisão e exemplo do comando API

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

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

Usando o comando da onda com `-o` a 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. Da informação nas credenciais de geração seção API, nós conhecemos o `clientID` e o `APIKey`, assim que esta seção do comando assemelhar-se-ia:

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

Em seguida, nós adicionamos o número de versão e o que nós gostaríamos de fazer. Para este exemplo nós executaremos as opções [GET /v1/computers](https://api.amp.sourcefire.com/v1/computers). O comando cheio olha como abaixo:

```
curl -o computers.json https://538e8b8203a48cc5c7fa:a190c911-8ca4-45fa-8740-e384ef2d3d5b@api.amp.sourcefire.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:a190c911-8ca4-45fa-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 incluem Windows: (Geralmente você querará 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.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"  
}
```

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

Documentos relacionados

- [Cisco ampère para a documentação dos valores-limite API](#)