

Configurar e Solucionar Problemas do Cliente da API do AppDynamics

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Criar um cliente de API](#)

[Exibir Cliente de API Existente](#)

[Excluir Cliente de API Existente](#)

[Gerar token de acesso](#)

[IU do administrador \(tokens de longa duração\)](#)

[API OAuth \(tokens de vida curta\)](#)

[Gerenciar tokens de acesso](#)

[Regenerar Token de Acesso](#)

[Revogar token de acesso](#)

[Usar token de acesso para criar API Rest](#)

[Problemas e soluções comuns](#)

[401Não autorizado](#)

[Resposta vazia.](#)

[Tipo de Conteúdo Inválido](#)

[Informações Relacionadas](#)

[Precisa de mais assistência?](#)

Introdução

Este documento descreve como criar um cliente da API do AppDynamics, gerar Tokens e solucionar problemas.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Para criar um Cliente de API, um Usuário deve ter a função Proprietário da conta (Padrão) ou uma função personalizada com a permissão Administração, Agentes, Assistente do Guia de Introdução.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Controlador AppDynamics

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

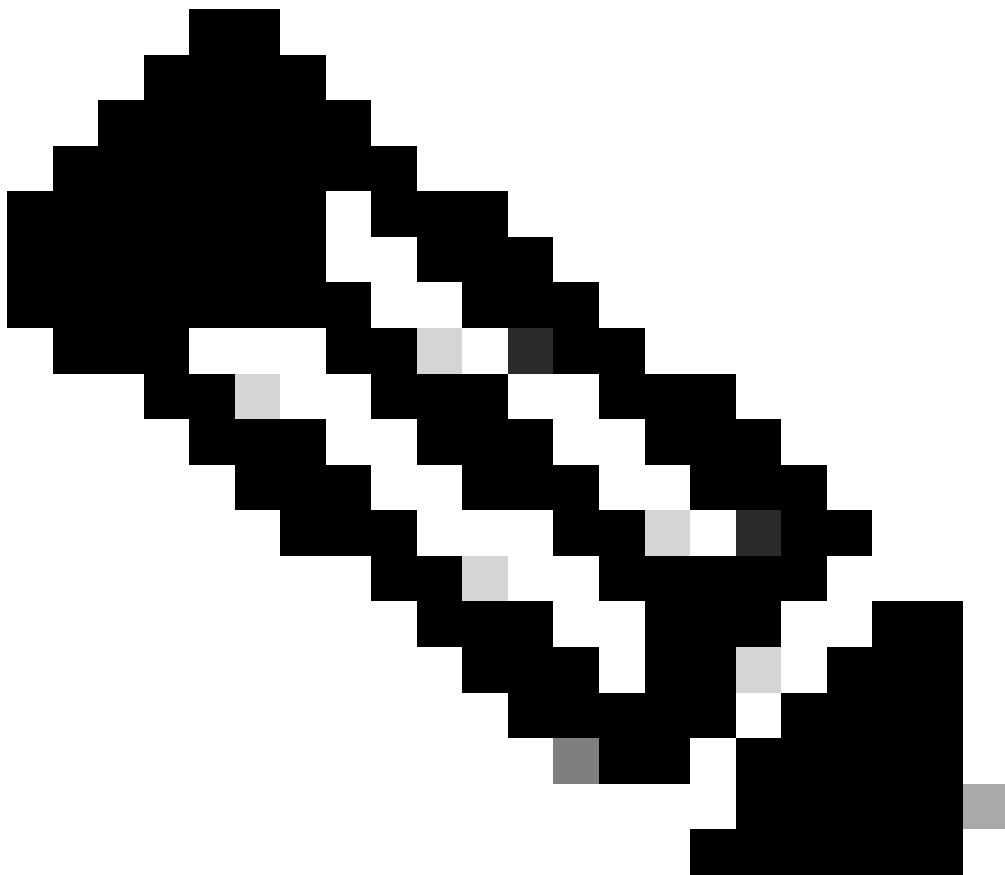
Informações de Apoio

Este documento descreve o processo de criação de Clientes de API para acessar com segurança os dados do AppDynamics Controller usando as chamadas de Transferência de Estado Representacional (REST) e Interface de Programação de Aplicativo (API). Os Clientes API utilizam autenticação baseada em token Open Authorization (OAuth). O OAuth permite que serviços de terceiros acessem informações de uma conta de usuário final sem expor as credenciais do usuário. Ele atua como um intermediário, fornecendo ao serviço de terceiros um token de acesso que autoriza o compartilhamento de informações específicas da conta. Os usuários podem gerar o token OAuth após configurar o Cliente de API. Além disso, este documento aborda a solução de problemas comuns encontrados durante o uso de Clientes API.

Configurar

Criar um cliente de API

1. Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma função com permissão de Administração, Agentes, Assistente de Introdução.
2. Clique em Nome de usuário (canto superior direito) > Administração.
3. Clique na guia Cliente API.
4. Clique em + Criar.
5. Insira o nome do cliente e a descrição.
6. Clique em Generate Secret para preencher o segredo do cliente.



Note: O segredo do cliente é gerado e exibido apenas uma vez. Copie e armazene essas informações com segurança.

7. Defina a Expiração do token padrão.
8. Clique em + Adicionar na seção Funções para adicionar a função.
9. Clique em Save na parte superior direita.

Exibir Cliente de API Existente

1. Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma função com permissão de Administração, Agentes, Assistente de Introdução.
2. Clique em Nome de usuário (canto superior direito) > Administração.
3. Clique na guia Cliente de API para exibir os Clientes de API existentes.

Excluir Cliente de API Existente

1. Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma

- função com permissão de Administração, Agentes, Assistente de Introdução.
2. Clique no Nome de usuário (canto superior direito) > Administração > Clientes API.
 3. Localize os clientes API específicos que deseja excluir e selecione-os.
 4. Clique no ícone Excluir ou Clique com o botão direito do mouse nos clientes da API selecionados e selecione Excluir clientes da API para excluir os clientes da API existentes.
-



aviso: A exclusão do Cliente de API invalida o token.

Gerar token de acesso

O Token de Acesso pode ser gerado por meio da IU do Administrador ou da API OAuth. A interface do usuário fornece tokens de vida longa, enquanto a API OAuth gera tokens de vida curta, atualizados regularmente.

- IU do administrador (tokens de longa duração)
 - Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma

função com permissão de Administração, Agentes, Assistente de Introdução.

- Clique no Nome de usuário (canto superior direito) > Administração > Clientes API.
- Selecione o cliente de API para o qual deseja gerar o token de acesso e clique em Gerar token de acesso temporário.
- Os tokens de acesso gerados pela interface do usuário têm um tempo de expiração maior.

- API OAuth (tokens de vida curta)

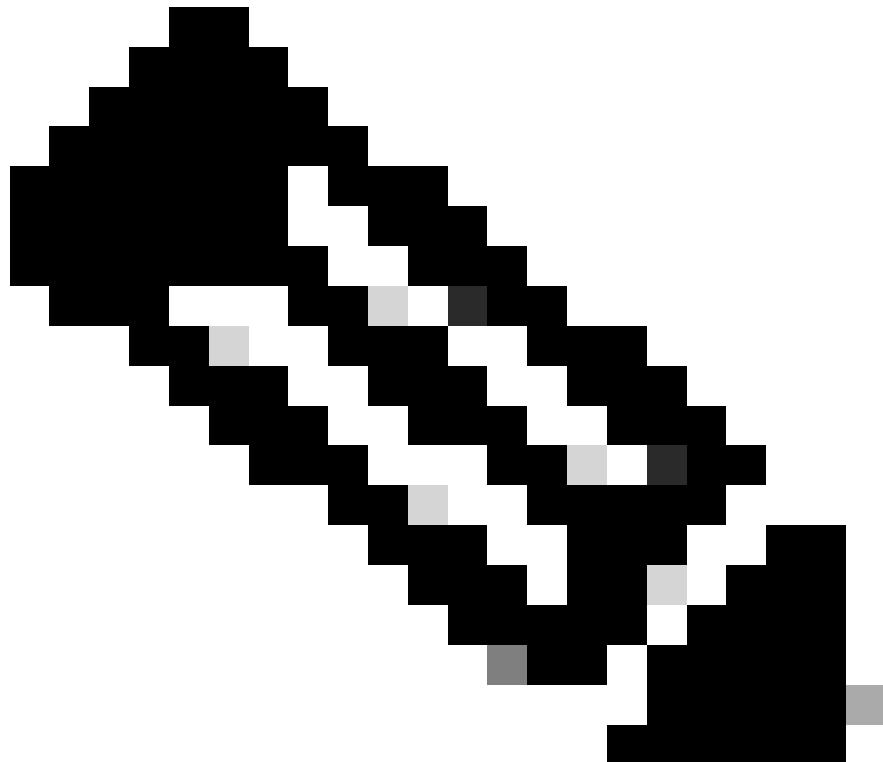
- `Você pode usar APIs REST para gerar um Token de Acesso de curta duração.

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" "https://  
  
/controller/api/oauth/access_token" -d 'grant_type=client_credentials&client_id=  
  
@  
  
&client_secret=  
  
,
```

Substituir:

- com o nome do cliente que você inseriu ao criar o cliente API ou como compartilhado pelo administrador.
- com o Nome da conta.
-

com o Segredo do Cliente que você gerou ao criar o Cliente API ou como compartilhado pelo administrador.



Note: O token sob demanda não é rastreado na interface do usuário.

Resposta de exemplo:

```
{
  "access_token": "

  ",
  "expires_in": 300
}
```

Gerenciar tokens de acesso

- Os tokens de acesso gerados a partir da API REST só podem ser invalidados com a exclusão do cliente da API associado.
- Os tokens de acesso gerados pela IU do controlador podem ser revogados ou regenerados.

- A regeneração de um token de acesso não invalida os tokens anteriores. Os tokens mais antigos permanecem ativos até sua expiração.
 - Não há como recuperar tokens anteriores ou válidos no momento. Portanto, somente o token atual pode ser revogado.
- Regenerar Token de Acesso
 - Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma função com permissão de Administração, Agentes, Assistente de Introdução.
 - Clique no Nome de usuário (canto superior direito) > Administração > Clientes API.
 - Selecione o API Client para o qual deseja gerar novamente o Access Token, clique em Regenerate > Save (canto superior direito).
 - Revogar token de acesso
 - Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma função com permissão de Administração, Agentes, Assistente de Introdução.
 - Clique em Nome de usuário (canto superior direito) > Administração > Clientes API.
 - Selecione o Cliente de API para o qual deseja Revogar o Token de Acesso, Clique em Revogar > Salvar (canto superior direito).

Usar token de acesso para criar API Rest

- De [APIs do AppDynamics de Splunk](#) determine o endpoint específico com o qual você precisa interagir.
- Construir a solicitação:
 - Método: Selecione o método HTTP (GET, POST, PUT, DELETE) com base na ação que deseja executar.
 - Cabeçalhos: adicione o token de acesso ao cabeçalho de autorização.
 - Corpo (se houver): Adicione o corpo da solicitação no formato JSON (JavaScript Object Notation).
- Exemplo de solicitação

```
curl --location --request GET 'https://
```

```
/controller/
```

```
' --header 'Authorization: Bearer
```

Substituir:

- com o URL do controlador.
- com o endpoint restante com o qual você precisa interagir.
- com o token de acesso gerado usando o nome do cliente e o segredo do cliente.

Problemas e soluções comuns

- 401 Não autorizado

- Problema: Os usuários encontram um erro 401 Unauthorized ao tentar gerar um token de acesso.
- Resposta de exemplo:

```
HTTP Error 401 Unauthorized
```

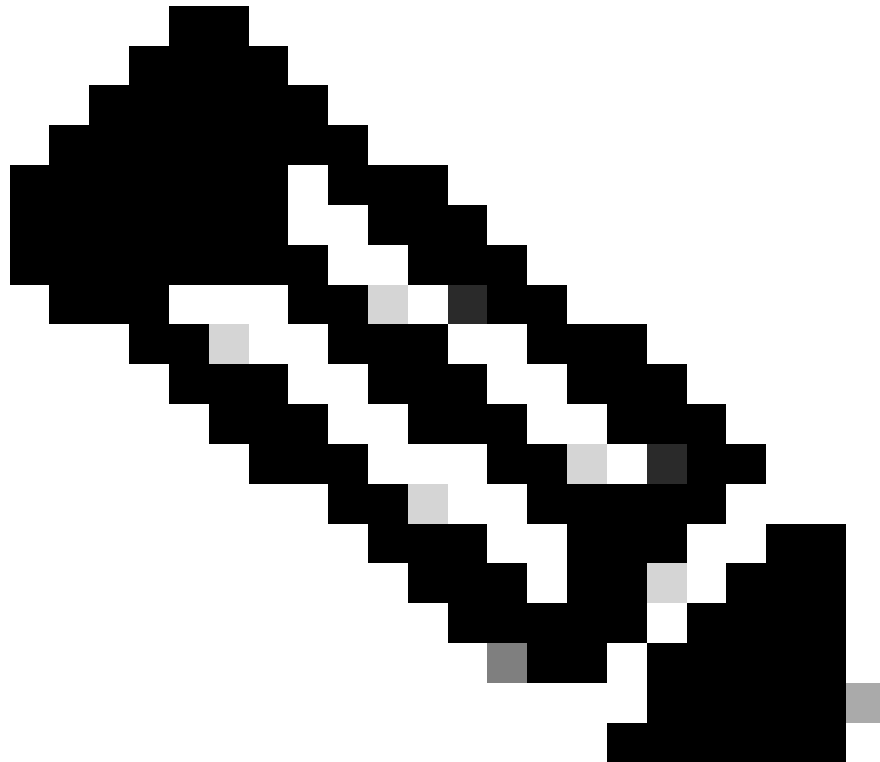
```
This request requires HTTP authentication
```

- Causa Raiz: O problema normalmente ocorre porque o segredo do cliente associado ao nome do cliente é inválido. Isso geralmente acontece quando o segredo do cliente é gerado, mas não salvo
- Solução:
 - Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma função com permissão de Administração, Agentes, Assistente de Introdução.
 - Clique em Nome de usuário (canto superior direito) > Administração.
 - Clique na guia Cliente de API para exibir os Clientes de API existentes.
 - Selecione o Cliente de API para o qual você está recebendo o erro.
 - Clique em Generate Secret para gerar um novo segredo do cliente e clique em

Save (canto superior direito)

- Resposta vazia.

- Problema: Os usuários encontram uma resposta vazia ao consultar um ponto de extremidade REST, mesmo depois de gerar um Token de Acesso com êxito.
- Resposta de exemplo:
- Causa raiz: O problema normalmente ocorre devido a funções ou permissões insuficientes atribuídas ao cliente da API. Sem as funções necessárias, o cliente API não pode recuperar os dados esperados do ponto de extremidade.
- Solução:
 - Faça login na IU do Controlador como uma Função de Proprietário da Conta ou uma função com permissão de Administração, Agentes, Assistente de Introdução.
 - Clique em Nome de usuário (canto superior direito) > Administração.
 - Clique na guia Cliente de API para exibir os clientes de API existentes.
 - Selecione o Cliente de API ao qual deseja atribuir a Função
 - Clique em + Adicionar na seção Funções para adicionar a função.
 - Clique em Save na parte superior direita.



Note: Certifique-se de que o cliente de API tenha as funções apropriadas atribuídas. As funções devem se alinhar com os requisitos de acesso a dados do ponto de extremidade REST.

- Tipo de Conteúdo Inválido

- Problema: O usuário encontrou um erro de Servidor Interno 500 ao tentar gerar um Token de Acesso.
- Exemplo de erro:

HTTP ERROR 500 javax.servlet.ServletException: java.lang.Illeg

- Causa raiz: O problema ocorre devido ao cabeçalho do tipo de conteúdo. Na versão 24.10 da controladora, o tipo de conteúdo foi alterado de `application/vnd.appd.cntrl+json;v=1` para `application/x-www-form-urlencoded`
 - Solução:
 - Modifique a solicitação e defina o cabeçalho do tipo de conteúdo como `application/x-www-form-urlencoded`
- Exemplo:

```
curl -X POST -H "Content-Type: application/x-www-form-urlencoded" "https://  
  
/controller/api/oauth/access_token" -d 'grant_type=client_credentials&client_id=  
  
@  
  
&client_secret=  
  
,
```

Informações Relacionadas

[Documentação do AppDynamics](#)

[APIs do AppDynamics Splunk](#)

[Clientes API](#)

[Gerenciar tokens de acesso](#)

Precisa de mais assistência?

Se você tiver uma dúvida ou estiver tendo problemas, crie um [tíquete de suporte](#) com estes detalhes:

- Detalhes do erro ou captura de tela: Forneça uma mensagem de erro específica ou uma captura de tela do problema.
- Comando usado: Especifique o comando exato que você estava executando quando o problema ocorreu.
- Server.log do controlador (somente no local): Se aplicável, forneça os registros do servidor da controladora em <controller-install-dir>/logs/server.log*

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.