

# Como: Recupere uma chave secreta do guarda-chuva perdida

## Objetivo

Se você já perdeu uma chave irrecuperável, você sabe quão rápido o sangue pode começar a bombear através do seu corpo. Este artigo mostrará como recuperar-se da perda da chave da API (Application Programming Interface, interface de programação de aplicativos) secreta. Essa chave secreta é exibida apenas uma vez quando gerada e não é exibida novamente. Se você navegar pelo navegador para fora da tela da chave API, poderá perder essas informações.

## Dispositivos aplicáveis

- WAP125
- WAP581

## Versão de software

- 1.0.1

## Requirements

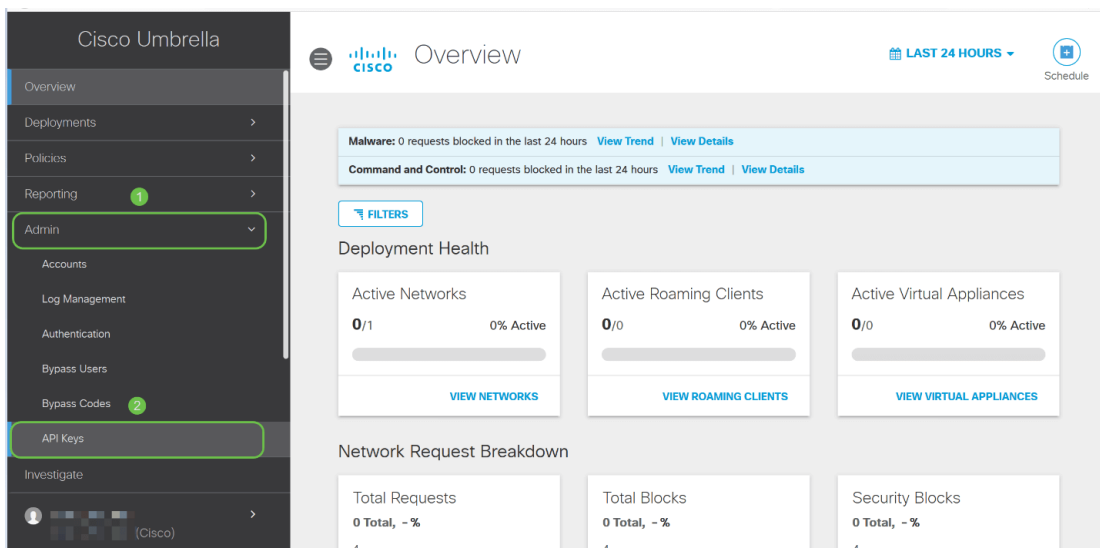
- Uma conta Umbrella ativa (não tem uma? [Solicitar um orçamento](#) ou iniciar uma [avaliação gratuita](#))

## Socorro, eu perdi minha chave secreta!

Aqui estão as notícias difíceis, a chave secreta, está perdida para a rede de éter, sumiu. Onde isto se transforma em melhores notícias, é que o processo de recuperação não é assim tão doloroso. Ao gerar uma nova chave API, você gera uma nova chave secreta. Portanto, o processo de recuperação envolve a exclusão da chave API associada à chave perdida e a geração do novo conjunto de chaves API.

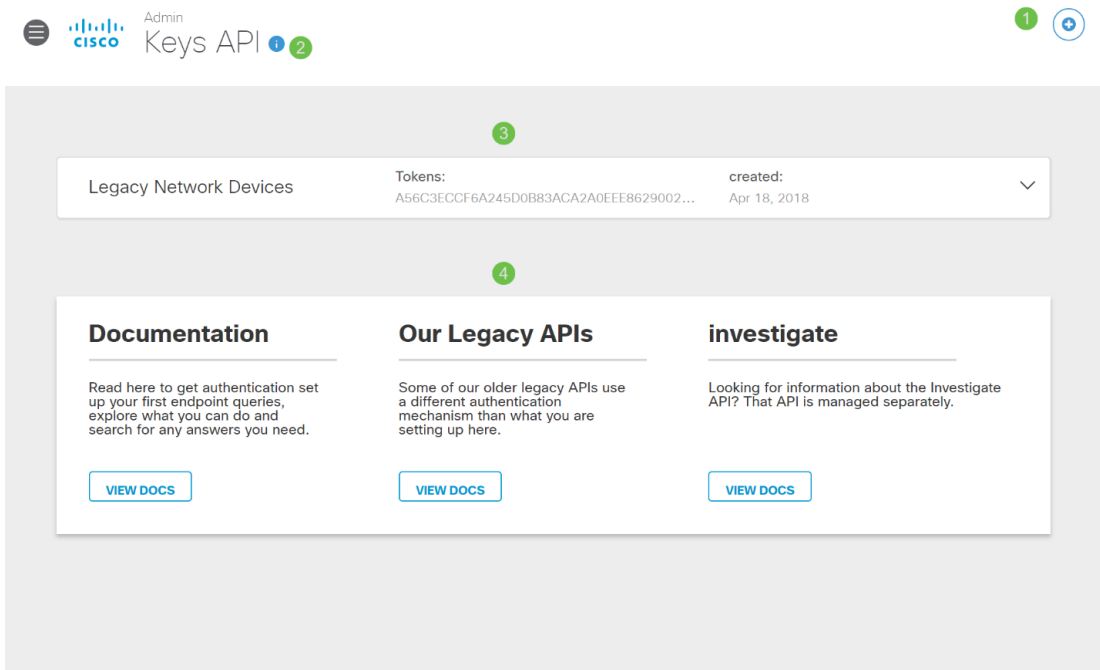
Onde este guia está navegando, começa com a captura da chave API e da chave Secret no painel da conta Umbrella. Depois disso, entraremos em seu dispositivo WAP para adicionar a API e a chave Secret. Se tiver problemas, [consulte aqui a documentação](#) e [aqui para ver as opções de suporte do Umbrella](#).

Etapa 1. Depois de fazer login em sua Conta Umbrella, na tela *Dashboard*, clique em **Admin > API Keys**.



## Anatomia da tela de chaves API -

1. *Add API Key* - Inicia a criação de uma nova chave para uso com a API Umbrella.
2. *Informações adicionais* - desliza para baixo/para cima com um explicador para esta tela.
3. *Token Well* - Contém todas as chaves e tokens criados por esta conta. (Preenche uma vez que uma chave foi criada)
4. *Documentos de suporte* - Links para a documentação no site Umbrella referente aos tópicos em cada seção.



Etapa 2. Clique no botão **Umbrella Network Devices** no *Token well*.



Legacy Network Devices	Token: A56	Created: Apr 18, 2018	▼
<b>Umbrella Network Devices</b>	Key: 494	Created: Aug 8, 2018	▼

### Documentation

Read here to get authentication set up for your first endpoint queries, explore what you can do and search for any answers you need.

[VIEW DOCS](#)

### Our Legacy APIs

Some of our older legacy APIs use a different authentication mechanism than what you are setting up here and have unique functions.

[VIEW DOCS](#)

### Investigate

Looking for information about the Investigate API? That API is managed separately.

[VIEW DOCS](#)

Etapa 3. Selecione **Umbrella Network Devices** e clique no botão **Create**.



Legacy Network Devices	Token: A56	Created: Apr 18, 2018	▼
<b>Umbrella Network Devices</b>	Key: 494	Created: Aug 8, 2018	▲

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

**Your Key:** 494: [key visualization]

Check out the [documentation](#) for step by step instructions.

[DELETE](#)

[REFRESH](#) [CLOSE](#)

Etapa 4. A chave será excluída instantaneamente. Clique no botão **Add API Key** (Adicionar chave de API) no canto superior direito ou clique no botão **Create API Key** (Criar chave de API). Ambos funcionam da mesma forma.



Legacy Network Devices
Token: A56
Created: Apr 18, 2018

### Documentation

Read here to get authentication set up for your first endpoint queries, explore what you can do and search for any answers you need.

[VIEW DOCS](#)

### Our Legacy APIs

Some of our older legacy APIs use a different authentication mechanism than what you are setting up here and have unique functions.

[VIEW DOCS](#)

### Investigate

Looking for information about the Investigate API? That API is managed separately.

[VIEW DOCS](#)

Etapa 5. Selecione **Umbrella Network Devices** e clique no botão **Create**.

## What should this API do?

Choose the API that you would like to use.

**Umbrella Network Devices**  
 To be used to integrate Umbrella-enabled hardware with your organization. In addition, allows you to create, update, list and delete identities in Umbrella.

**Legacy Network Devices**  
 A Network Devices token enables hardware network devices such as Cisco Wireless Lan Controllers and Cisco Integrated Services Routers 4000 series to integrate with Umbrella.  
ⓘ You can only generate one token. Refresh your current token to get a new token.

**Umbrella Reporting**  
 Enables API access to query for Security Events and traffic to specific Destinations

CANCEL CREATE

Etapa 6. Clique no botão **Copiar** à direita de sua *Chave secreta*; uma notificação pop-up confirmará que a chave foi copiada para sua área de transferência.

Umbrella Network Devices
Key: aae
Created: Jul 26, 2018

The API key and secret here are used to perform API requests against your Umbrella organization, such as identity management, reporting and more. If you are using an Umbrella-integrated hardware device that uses basic authentication, this allows management of Umbrella from the device and vice versa.

**Your Key:** aae

**Your Secret:** 352

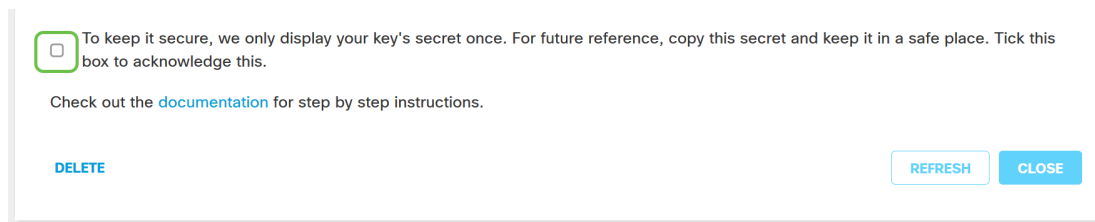
To keep it secure, we only display your key's secret once. For future reference, copy this secret and keep it in a safe place. Tick this box to acknowledge this.

Check out the [documentation](#) for step by step instructions.

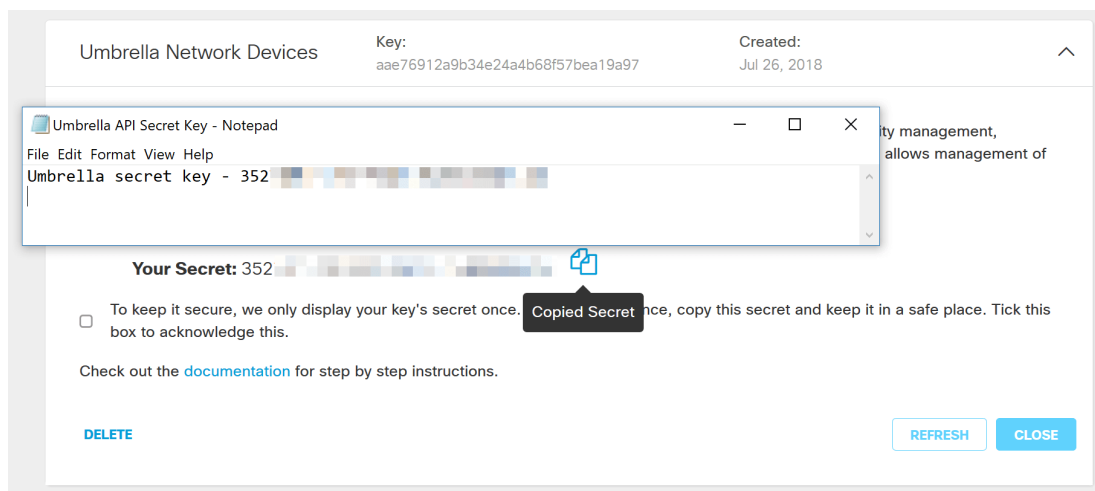
DELETE
REFRESH
CLOSE

Depois de copiar a chave e a chave secreta em um local seguro, clique na **caixa de seleção** para

confirmar a confirmação completa e clique no botão **Fechar**.



Passo 7. Abra um editor de texto, como o bloco de notas, cole sua chave secreta e API no documento, rotule-o para referência futura. Neste caso, a etiqueta é "Chave secreta dos Guarda-chuvas". Inclua a chave API com sua chave secreta, juntamente com uma breve descrição de seu uso neste mesmo arquivo de texto. Em seguida, salve o arquivo de texto em um local seguro que será fácil de acessar mais tarde, se você precisar.



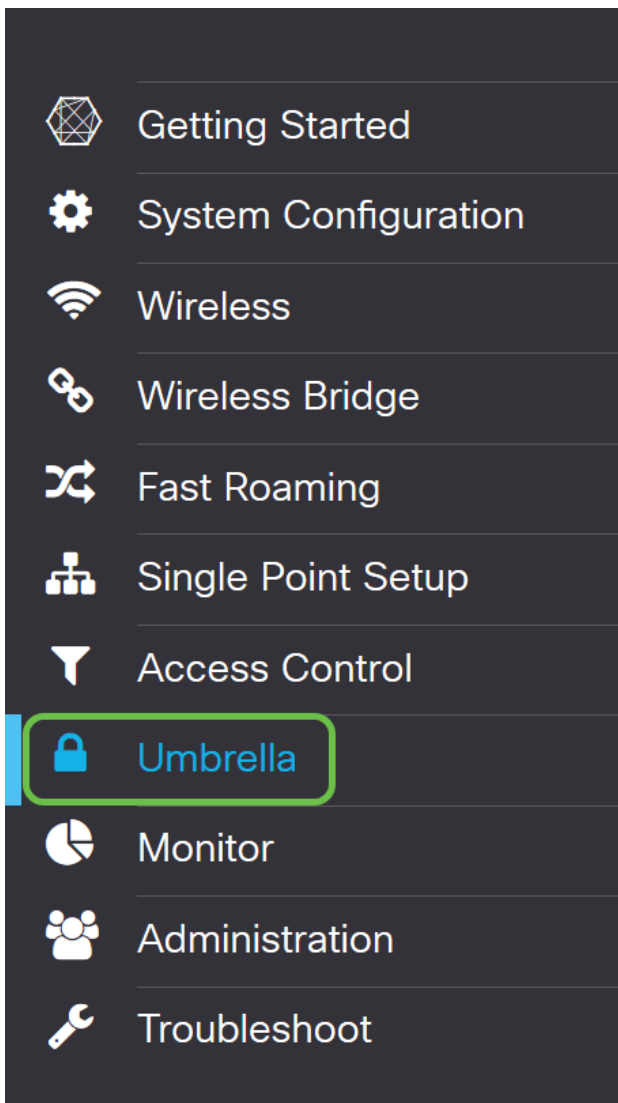
**Nota importante:** Se você perder ou excluir acidentalmente a chave secreta, não há nenhuma função ou número de suporte para chamar para recuperar essa chave. [Guarde segredo](#). Se perdido, você precisará excluir a chave e reautorizar a chave API com cada dispositivo WAP que deseja proteger com o Umbrella.

**Prática recomendada:** Mantenha apenas uma *única* cópia deste documento em um dispositivo, como um pen drive USB, inacessível de qualquer rede.

## Configurando o Umbrella em seu dispositivo WAP

Agora que criamos chaves API dentro do Umbrella, pegamos essas chaves e as instalamos em nossos dispositivos WAP. Em nosso caso, estamos usando um WAP581.

Etapa 1. Depois de fazer login em seu dispositivo WAP, clique em **Umbrella** no menu da barra lateral.



Etapa 2. A tela Umbrella é direta, mas há dois campos que merecem ser definidos aqui:

- *Domínios locais a serem ignorados* - Este campo contém seus domínios internos que você gostaria de excluir do serviço Umbrella.
- *DNSCrypt* - Protege a transferência de pacotes entre o cliente DNS e o DNS Resolver. Esse recurso está ativado por padrão. Desabilitar esse recurso tornará sua rede menos segura.

The screenshot shows the Cisco Umbrella configuration interface. At the top, there's a header with the Cisco logo, the device name 'WAP581-WAP581', and a language dropdown set to 'English'. Below the header, the title 'Umbrella' is displayed with 'Save' and 'Cancel' buttons. The main content area contains a brief description of Cisco Umbrella and instructions on integration. Below this, there are several configuration fields: 'Enable' (checkbox), 'API Key' (text input), 'Secret' (text input), 'Local Domains to Bypass (optional)' (text input with placeholder 'Multiple inputs separated by comma'), 'Device Tag (optional)' (text input with value 'WAP581'), 'DNSCrypt' (checkbox with label 'Enable'), and 'Registration Status'.

Etapa 3. Cole sua API e chave secreta nos campos correspondentes

**Umbrella** Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.  
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.  
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

Etapa 4. Verifique se as caixas de seleção de **Enable** e **DNSCrypt** estão alternadas para o estado de verificação.

**Umbrella** Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.  
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.  
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

DNSCrypt:  Enable

Registration Status:

**Note:** O DNSCrypt protege a comunicação DNS entre um cliente DNS e um resolvedor DNS. O padrão está ativado.

Etapa 5. (Opcional) Insira os domínios locais que deseja que o Umbrella permita por meio do processo de resolução de DNS.

**Umbrella** Save Cancel

Cisco Umbrella is a cloud security platform that provide the first line of defense against threats on the internet wherever users go.  
With an [Umbrella account](#), this integration will transparently intercept DNS queries and redirect them to Umbrella.  
This device will appear in the [Umbrella dashboard](#) as a network device for applying policy and viewing reports.

Enable:

API Key:

Secret:

Local Domains to Bypass (optional):

Device Tag (optional):

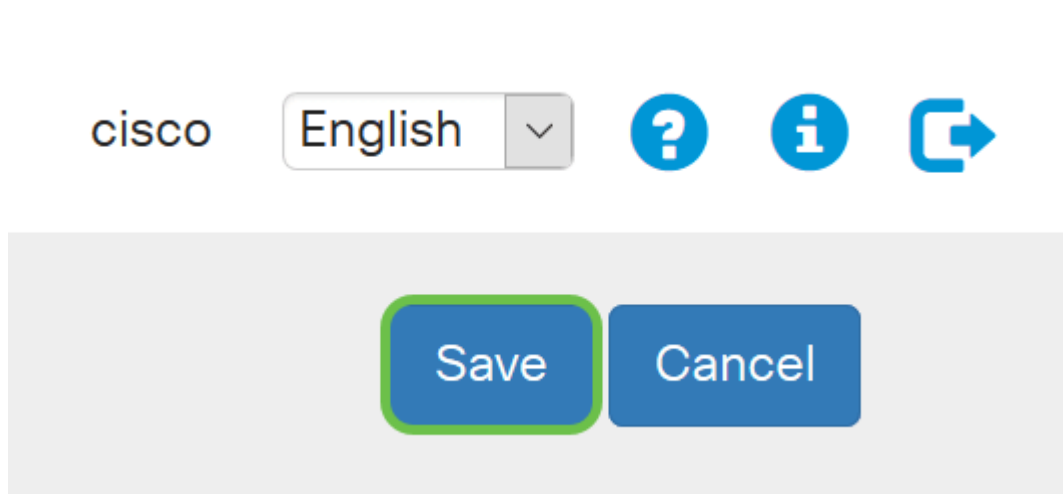
DNSCrypt:  Enable

Registration Status:

**Note:** Isso é necessário para todos os domínios de intranet e domínios DNS divididos. Se a sua rede exigir o uso de domínios de área local para roteamento, você precisará entrar em contato

com o suporte do Umbrella para ativar e executar esse recurso. A maioria dos usuários não precisará usar essa opção.

Etapa 6. Depois de estar satisfeito com as alterações ou ter adicionado seus próprios *domínios locais para ignorar*, clique no botão **Salvar** no canto superior direito.



Passo 7. Quando as alterações forem concluídas, o campo *Status do registro* exibirá "Êxito".

A screenshot of the Cisco Umbrella configuration page. The page contains several fields and checkboxes. The "Enable:" checkbox is checked. The "API Key:" field contains the text "aae" followed by a blurred area. The "Secret:" field contains the text "352" followed by a blurred area. The "Local Domains to Bypass (optional):" field contains the text "Multiple inputs separated by comma". The "Device Tag (optional):" field contains the text "WAP581". The "DNSECrypt:" checkbox is checked and labeled "Enable". At the bottom, the "Registration Status:" field is highlighted with a green border and displays the text "Successful".

## Confirmando que tudo está no lugar certo

Parabéns, agora você está protegido com o Umbrella da Cisco. Ou você é? Vamos ter certeza de que a Cisco criou um site dedicado a determinar isso tão rapidamente quanto a página é carregada. [Clique aqui](#) ou digite <https://InternetBadGuys.com> na barra do navegador.

Se o Umbrella estiver configurado corretamente, você será saudado por uma tela semelhante a esta!





**SECURITY THREAT DETECTED AND BLOCKED**

Based on Cisco Umbrella security threat information, access to the web site **Not\_Found** has been blocked to prevent an attack on your browser.

Malware protection has shifted from the endpoint, deeper into the network, in order to cater to a growing number and variety of devices. In order to offer the most effective protection to computing assets on the Cisco network, Infosec, Cisco IT, and the Security Business Group have jointly rolled out Umbrella protection for Cisco's corporate DNS infrastructure. This service will block access to hostnames that are known bad and has been deployed to prevent malicious actors from serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this page should not be blocked, [open a case](#) providing the following information:

- Text or screenshot of the corresponding debug information below
- Business justification for use of the website

**Block Reason: Umbrella DNS Block**

Date: July 26, 2018  
Time: 22:58:17  
Host Requested: Not\_Found  
URL Requested: Not\_Found  
Client IP address: [redacted]  
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:61.0) Gecko/20100101 Firefox/61.0  
Request Method: GET