

如何：恢复丢失的Umbrella密钥

目标

如果你丢失了不可恢复的密钥，你知道血能多快地开始流进你的身体。本文将介绍如何从丢失机密应用程序编程接口(API)密钥中恢复。此密钥在生成时仅显示一次，不再显示。如果从API密钥屏幕导航浏览器，则可能会丢失该信息。

适用设备

- WAP125
- WAP581

软件版本

- 1.0.1

要求

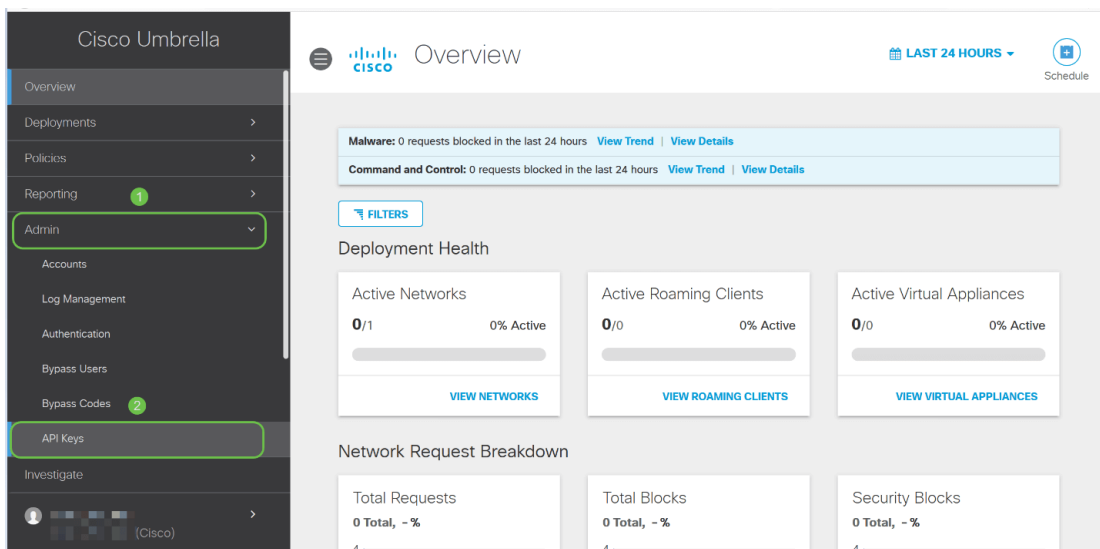
- 活动的Umbrella帐户(没有？[请求报价](#)或开始[免费试用](#))

救命，我的密钥丢了！

这是个坏消息，你的密钥，它被以太网丢失了。而如果这变成更好的消息，那就是复苏过程并不那么痛苦。通过生成新的API密钥，可生成新的密钥。因此，恢复过程包括删除与丢失密钥关联的API密钥并生成新的API密钥集。

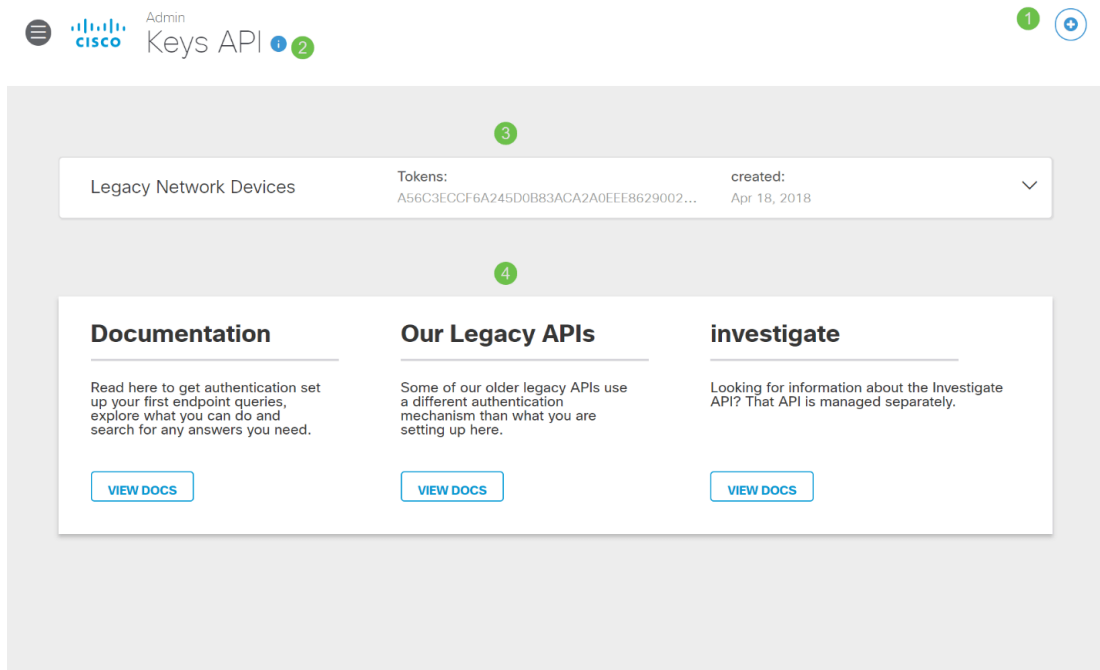
在本指南导航的位置，首先从Umbrella帐户控制面板获取API密钥和密钥。之后，我们将登录您的WAP设备以添加API和密钥。如果遇到任何问题，请[查看此处获取文档](#)，并[查看此处获取Umbrella Support选项](#)。

步骤1.登录Umbrella帐户后，从Dashboard屏幕单击Admin > API Keys。

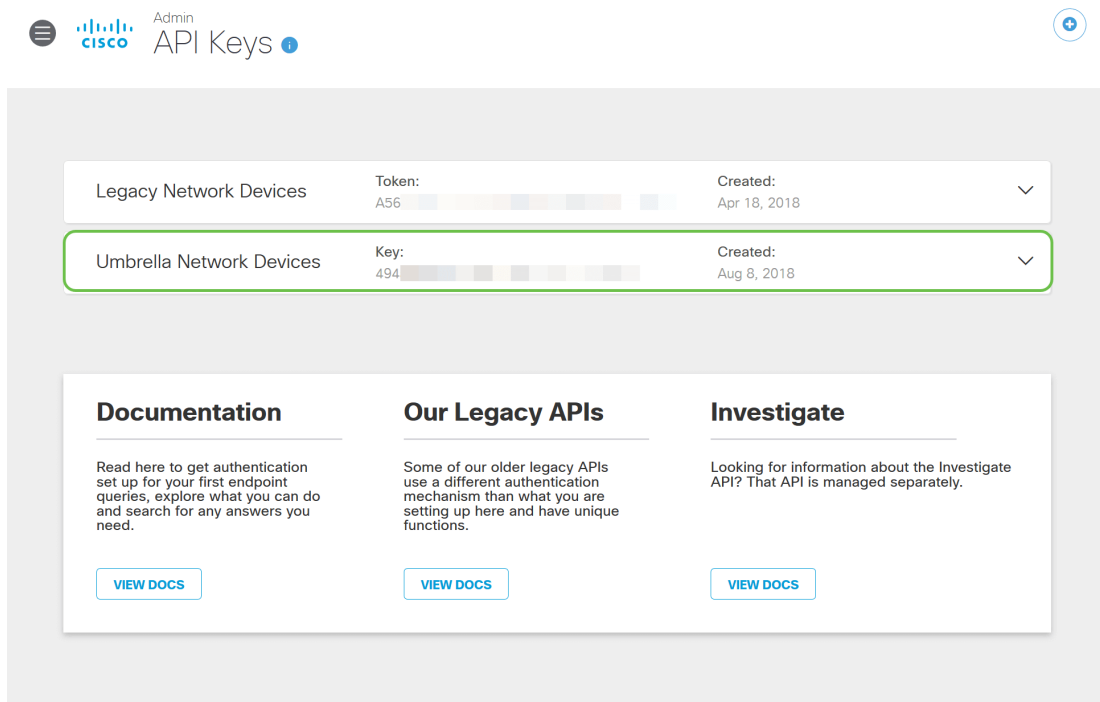


API密钥剖析屏幕 —

1. **Add API Key** — 启动新密钥的创建，以便与Umbrella API一起使用。
2. **其他信息** — 向下/向上滑动，其中包含此屏幕的说明者。
3. **令牌良好** — 包含此帐户创建的所有密钥和令牌。（创建密钥后填充）
4. **支持文档** — 链接到Umbrella站点上与每个部分中的主题相关的文档。



步骤2.单击令牌中的**Umbrella Network Devices**按钮，查看。



步骤3.选择**Umbrella Network Devices**，然后单击“**创建**”按钮。



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

Umbrella Network Devices 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: [masked]

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

DELETE **REFRESH** **CLOSE**

步骤4. 密钥将立即删除。单击右上角的Add API Key (添加API密钥) 按钮，或单击Create API Key(创建API密钥)按钮。它们的功能相同。



Admin API Keys

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

步骤5. 选择Umbrella Network Devices，然后单击“创建”按钮。

What should this API do?

Choose the API that you would like to use.

1



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.

i 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


2


CREATE

步骤6.单击“密钥”右侧的“复制”按钮，弹出通知将确认密钥已复制到剪贴板。

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**

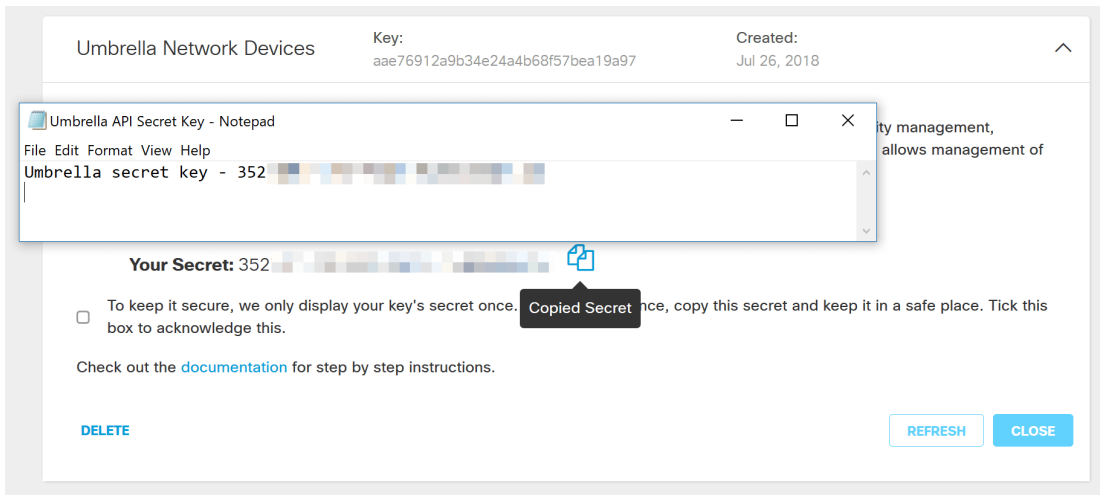
将密钥和密钥复制到安全位置后，单击复选框以确认完成确认，然后单击“关闭”按钮。

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**

步骤7.打开文本编辑器（如记事本），将您的密钥和API密钥粘贴到文档中，并标记它们以备将来参考。在本例中，其标签为“Umbrella secret key”。将API密钥与密钥一起包含，并简要说明其在同一文本文件中的用途。然后，将文本文件保存到安全位置，以便您稍后根据需要轻松访问。



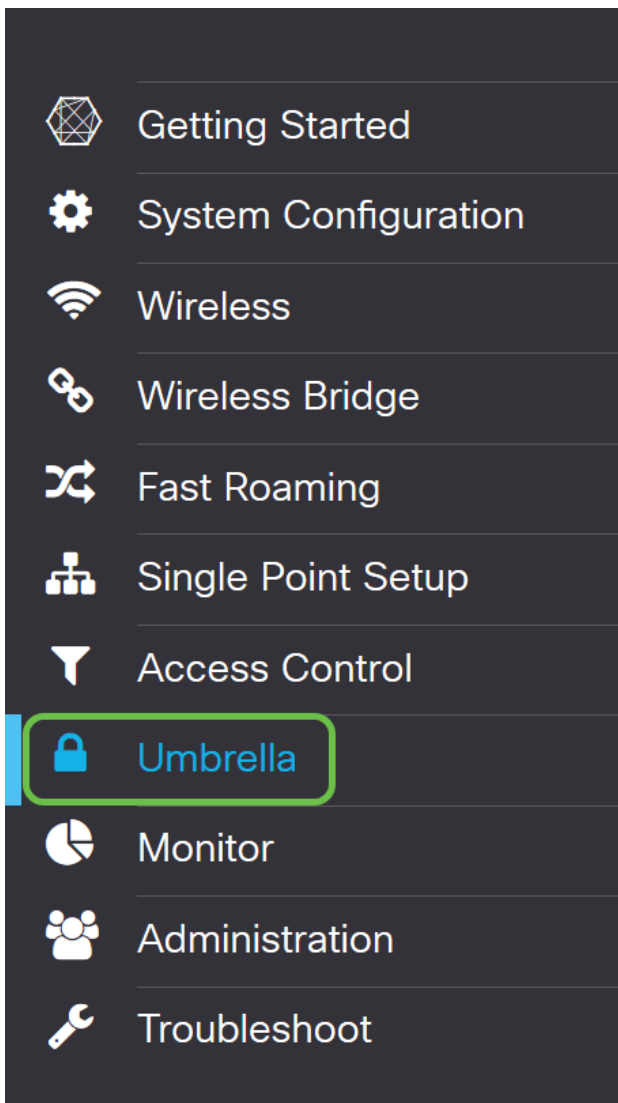
重要说明：如果丢失或意外删除了密钥，则没有功能或支持号码可供调用以检索此密钥。[保密，保密](#)。如果丢失，您需要删除密钥，并对您希望使用Umbrella保护的每个WAP设备重新授权API密钥。

最佳实践:在设备(如USB闪存)上只保留一份本文档的副本，不能从任何网络访问。

在WAP设备上配置Umbrella

现在，我们已在Umbrella中创建了API密钥，我们将获取这些密钥并将其安装在WAP设备上。在本例中，我们使用WAP581。

步骤1.登录WAP设备后，单击侧栏菜单中的Umbrella。



步骤2. Umbrella屏幕非常简单，但此处有两个值得定义的字段：

- **要绕行的本地域** — 此字段包含要从Umbrella服务中排除的内部域。
- **DNSCrypt** — 保护DNS客户端和DNS解析器之间的数据包传输。此功能默认启用，禁用此功能会降低网络的安全性。

The image shows the Cisco Umbrella configuration page for a device named WAP581-WAP581. The page has a light gray background and a white header with the Cisco logo and the device name. On the right side of the header, there are links for 'cisco', a language dropdown set to 'English', and icons for help, information, and share. The main content area is titled 'Umbrella' and contains a 'Save' button and a 'Cancel' button. Below the title, there is a paragraph of text explaining the integration: '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.' The configuration fields are: 'Enable:' with an unchecked checkbox; 'API Key:' with a text input field; 'Secret:' with a text input field; 'Local Domains to Bypass (optional):' with a text input field containing 'Multiple inputs separated by comma'; 'Device Tag (optional):' with a text input field containing 'WAP581'; 'DNSCrypt:' with an unchecked checkbox labeled 'Enable'; and 'Registration Status:' with no visible input.

步骤3.将API和密钥粘贴到相应的字段

WAP581-WAP581

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:

步骤4. 确保Enable和DNSCrypt的复选框已切换到选中状态。

WAP581-WAP581

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:

注意：DNSCrypt保护DNS客户端和DNS解析器之间的DNS通信。默认为启用。

步骤5. (可选) 输入您希望Umbrella允许通过DNS解析过程的本地域。

WAP581-WAP581

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:

注意：所有内部网域和拆分DNS域都需要此功能。如果您的网络需要使用局域网进行路由，则需要联系Umbrella支持人员以启动并运行此功能。大多数用户不需要使用此选项。

步骤6. 在您对更改感到满意或将自己的本地域添加到绕行后，单击右上角的保存按钮。

cisco


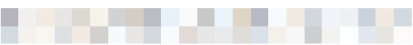


English



Save

Cancel

步骤7.完成更改后，Registration Status字段将显示为“Successful”。

Enable:	<input checked="" type="checkbox"/>
API Key: 	aae 
Secret: 	352 
Local Domains to Bypass (optional):	Multiple inputs separated by comma
Device Tag (optional):	WAP581
DNSEncrypt:	<input checked="" type="checkbox"/> Enable
Registration Status:	Successful

确认一切都在正确位置

祝贺您，您现在受到思科雨伞的保护。还是你？我们确信，思科已创建了一个网站，专门用于在页面加载时快速确定这一点。[单击此处](#)或在浏览器栏中键入<https://InternetBadGuys.com>。

如果Umbrella配置正确，您将看到类似此的屏幕！



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