

通过RV34x系列路由器配置网络上的Cisco Umbrella

简介

从固件版本1.0.0.2.16开始，RV34x系列路由器现在支持Cisco Umbrella。Umbrella使用DNS作为防御媒介或防御措施来防御恶意软件和数据入侵。

适用设备

- RV34x系列路由器

软件版本

- 1.0.02.16

要求

- 有效的Umbrella帐户(没有帐户？[申请报价](#)或开始[免费试用](#))

目标

本指南将向您展示将Umbrella的安全平台集成到您的网络中所涉及的步骤。在详细了解细节之前，我们将回答您可能要问自己的一些有关Umbrella的问题。

什么是umbrella?

Umbrella是思科提供的一个简单但非常有效的云安全平台。Umbrella在云中运行并执行许多安全相关服务。从突发威胁到事后调查Umbrella可发现并阻止跨所有端口和协议的攻击。

此计划如何运作？

Umbrella使用DNS作为防御的主要媒介。当用户在其浏览器栏中输入URL并点击Enter时，Umbrella会参与传输。该URL会传递到Umbrella的DNS解析器，如果安全警告与域关联，则请求会被阻止。此遥测数据传输和分析在微秒内完成，几乎不会增加延迟。遥测数据使用日志和仪器，跟踪全世界数十亿个DNS请求。当这些数据无处不在时，在全球范围内将其关联起来，可以在攻击开始时迅速做出响应。有关详细信息，请参阅思科的隐私政策 — [完整策略](#)、[摘要版本](#)。将遥测数据视为源自工具和日志的数据。

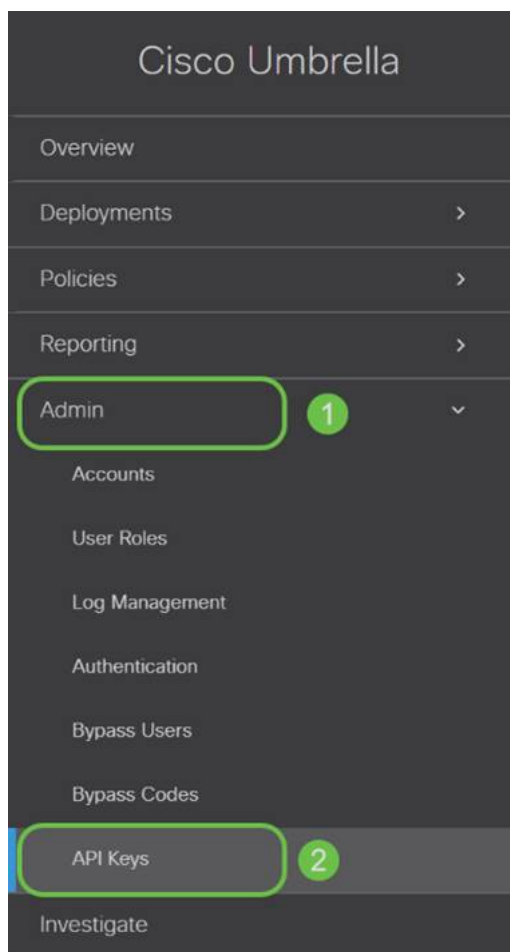
打个比方，想象你在一个派对上。在派对上，所有人都在打电话，在网上冲浪。在静默的集体沉默中，不时被参加派对的人点击屏幕打断。[这并不是一个很棒的派对](#)，但是在自己的手机上，你可以看到一张看起来让人无法抗拒的小猫GIF动画的超链接。但是，该URL似乎有问题，因此您不确定是否应该点击。因此，在点击超链接之前，您会向其他用户喊出“此链接是否损坏？”如果派对上的另一个人去过链接，发现这是骗局，他们会大喊，“是啊，我去了，这是

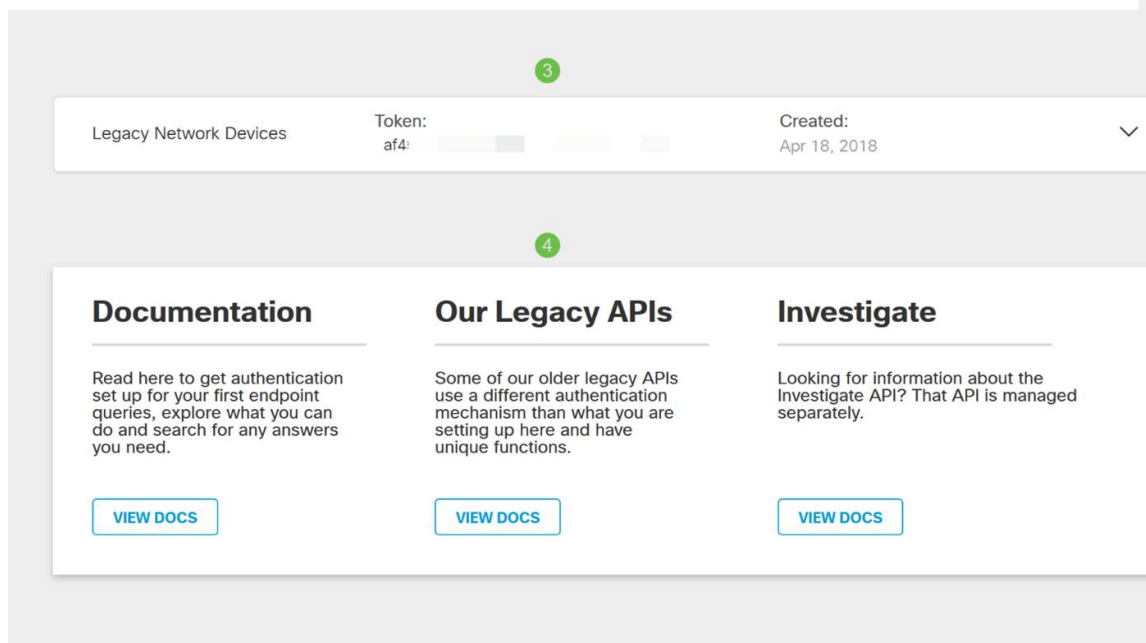
骗局！”你感谢他拯救你，继续你高贵地追寻可爱动物的图片。当然，在思科的规模下，这种类型的请求和回拨安全检查每秒会进行数百万次，这对您的网络安全性很有好处。

听起来很棒，我们怎么开始呢？

在本指南的导航位置，首先从您的Umbrella帐户控制面板获取API密钥和密钥。之后，我们将登录您的路由器设备以添加API和密钥。如果您遇到任何问题，请[在此处查阅文档](#)，并[在此处查看Umbrella支持选项](#)。

步骤1. 登录您的Umbrella帐户后，从Dashboard屏幕点击Admin > API Keys。

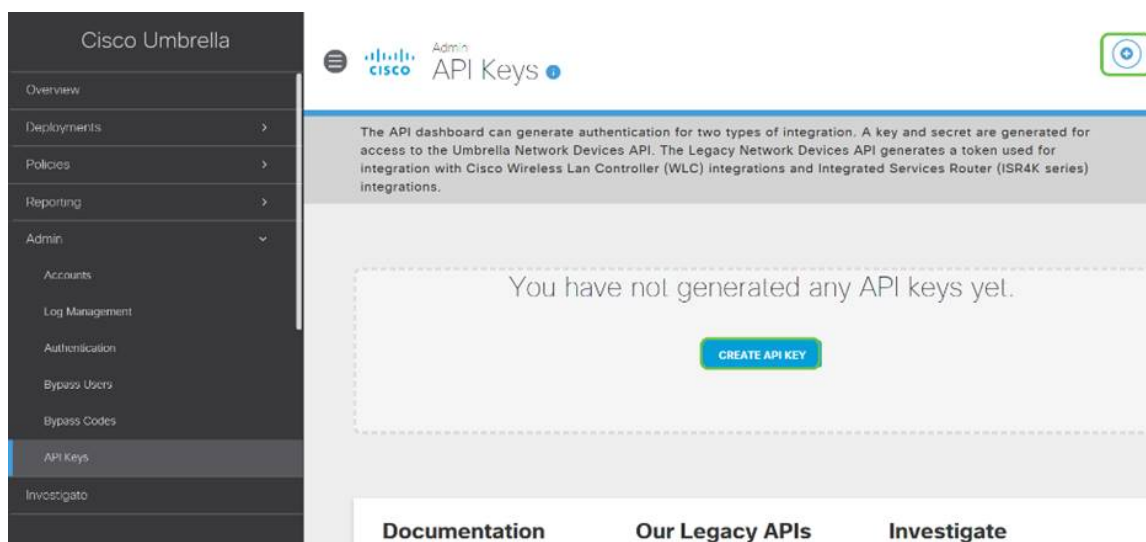




API密钥屏幕剖析（使用先前存在的API密钥） —

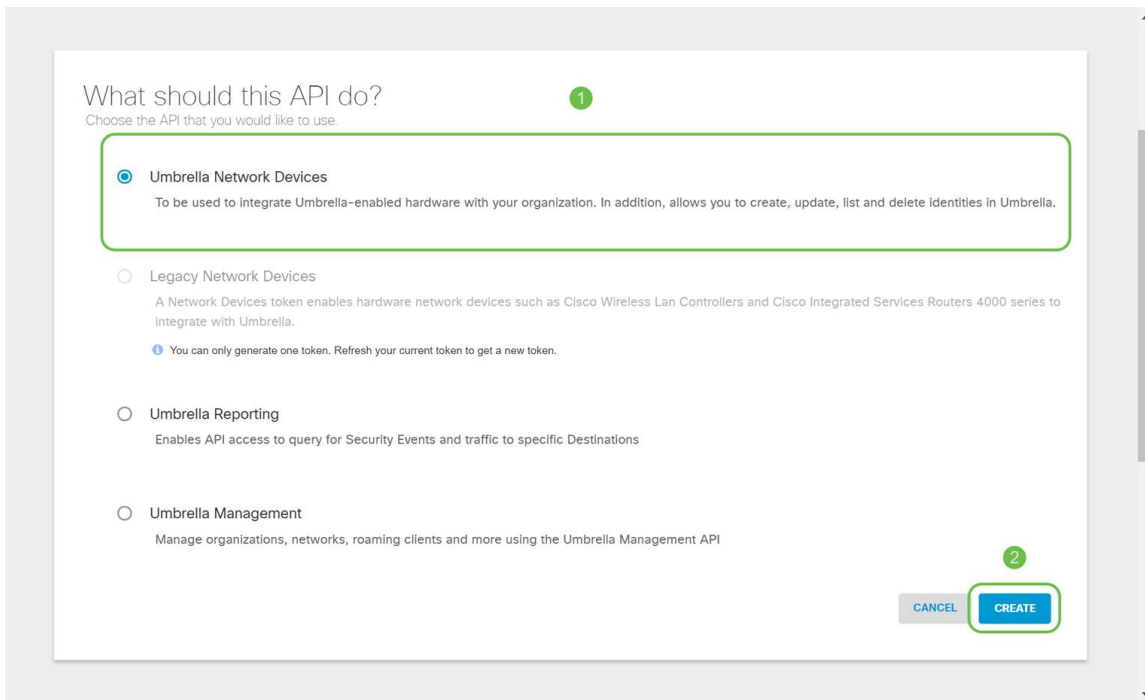
1. 添加API密钥 — 启动创建新密钥以与Umbrella API一起使用。
2. 附加信息 — 向下/向上滑动，并提供此屏幕的解释程序。
3. 令牌井 — 包含此帐户创建的所有密钥和令牌。（在创建密钥后填充）
4. 支持文档 — 链接至与每个部分中的主题相关的Umbrella站点文档。

步骤2. 点击右上角的**Add API Key**按钮，或点击**Create API Key**按钮。两者功能相同。

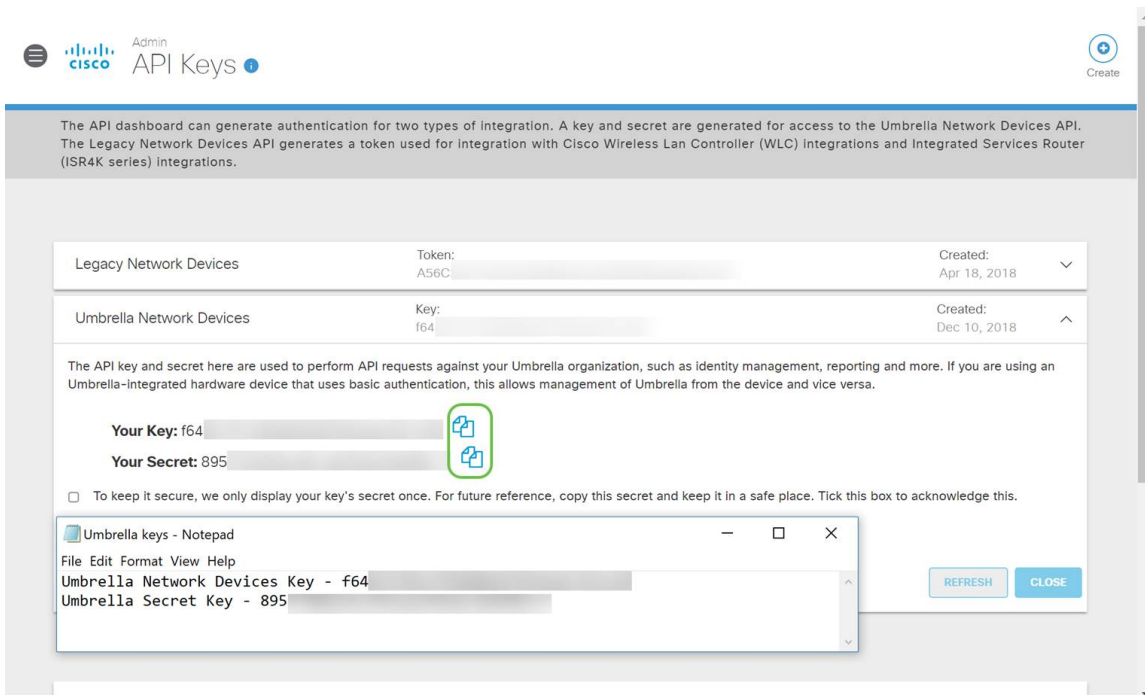


注意：上面的屏幕截图与您第一次打开此菜单时看到的类似。

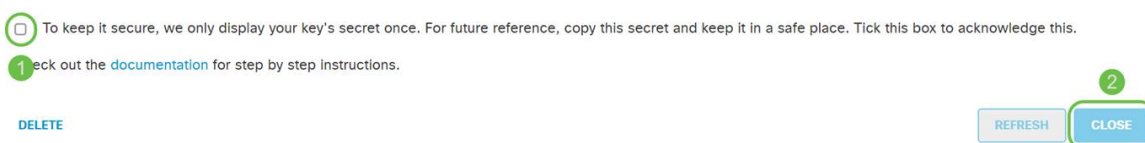
步骤3. 选择**Umbrella Network Devices**，然后单击**Create**按钮。



步骤4.打开文本编辑器（如记事本），然后单击API和API密钥(*Secret Key*)右侧的Copy按钮，弹出通知将确认密钥是否复制到剪贴板。一次一个将您的密钥和API密钥粘贴到文档中，并标记它们以供将来参考。在本例中，其标签为“Umbrella network devices key”。然后，将文本文件保存到安全位置，以便稍后访问。



步骤5.将密钥和密钥复制到安全位置后，从Umbrella API屏幕中单击复选框以确认完成对临时查看密钥的确认，然后单击Close按钮。



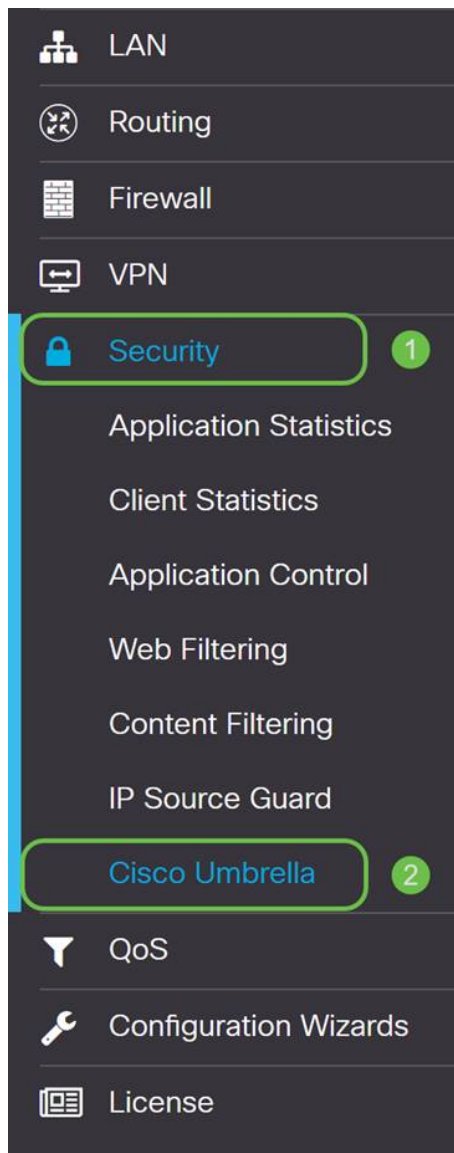
重要说明：如果丢失或意外删除了密钥，则没有函数或支持号码可供调用以检索此密钥。[保守秘密，保守安全](#)。如果丢失，您需要删除密钥，并对您希望使用Umbrella保护的每台设备重新授权新的API密钥。

最佳实践:在设备(如USB闪存)上只保留一份本文档的副本，任何网络都无法访问。

在RV34x设备上配置Umbrella

现在，我们已经在Umbrella内创建了API密钥，我们将使用这些密钥并将其安装到RV34x设备上。我们使用RV340。

步骤1. 登录到RV34x设备后，单击侧栏菜单中的**Security > Umbrella**。



步骤2. Umbrella API屏幕包含一系列选项，通过点击**Enable**（启用）复选框开始启用Umbrella。



Cisco Umbrella

Cisco Umbrella is a cloud security platform that provides 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.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
 - Go to [DNS-O-MATIC](#) website, create an account and add your OpenDNS account to it.
 - Go to [DNS-O-MATIC Settings](#) to enable DNS-O-MATIC so your WAN IP change can be propagated to O

Advanced Configuration

Local Domain To Bypass
(Optional):



DNSEncrypt:

Enable

Public Key:

B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8

- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

步骤3. (可选) 默认情况下, 选中Block LAN DNS Queries (阻止LAN DNS查询) 框, 此功能会自动在您的路由器上创建访问控制列表, 以防止DNS流量传出互联网。此功能强制所有域转换请求通过RV34x转发, 对大多数用户来说是一个好主意。

步骤4. 下一步有两种不同的方式。它们都取决于网络的设置。如果您使用DynDNS或NoIP等服务, 您将保留默认命名方案“Network”。然后, 您需要登录这些帐户, 以确保Umbrella在提供保护时与这些服务进行交互。出于我们依赖“网络设备”的目的, 请点击底部的单选按钮。



Cisco Umbrella

Apply

Cancel

Cisco Umbrella is a cloud security platform that provides 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.

- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

- If you use "Network" as this router's identity.
- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

步骤5. 现在单击Getting Started启动微型向导。

Cisco Umbrella

Apply Cancel

Cisco Umbrella is a cloud security platform that provides 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.

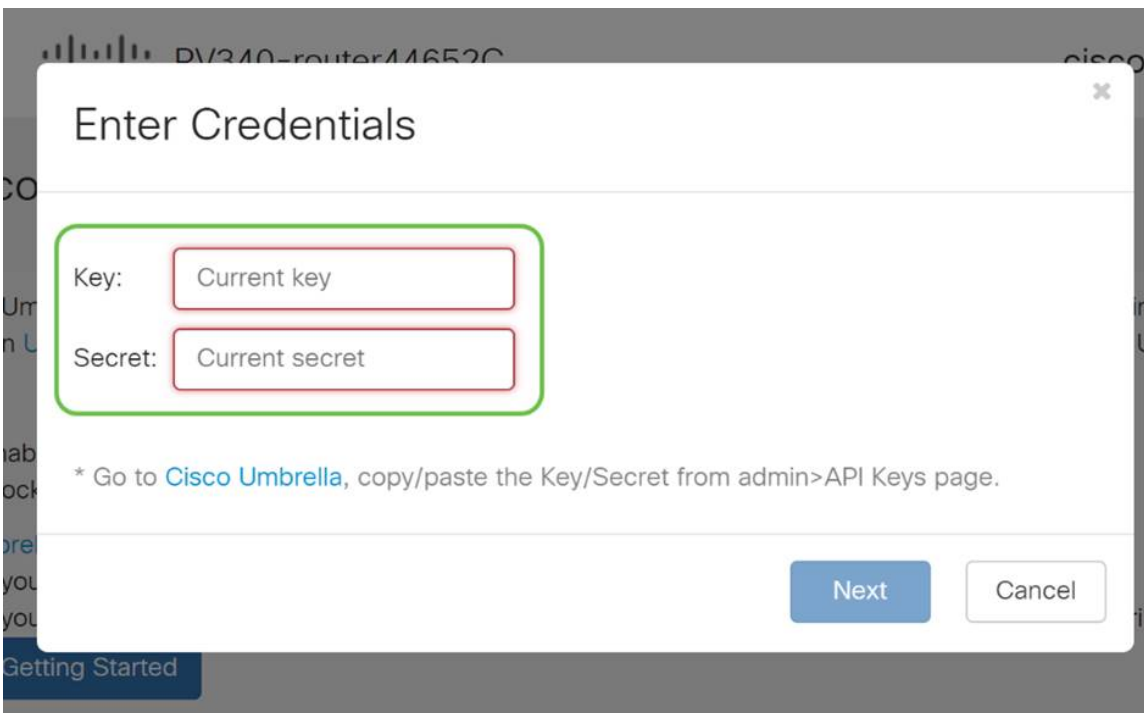
- Enable
- Block LAN DNS query

In [Umbrella Dashboard](#), you can create policies for different identities:

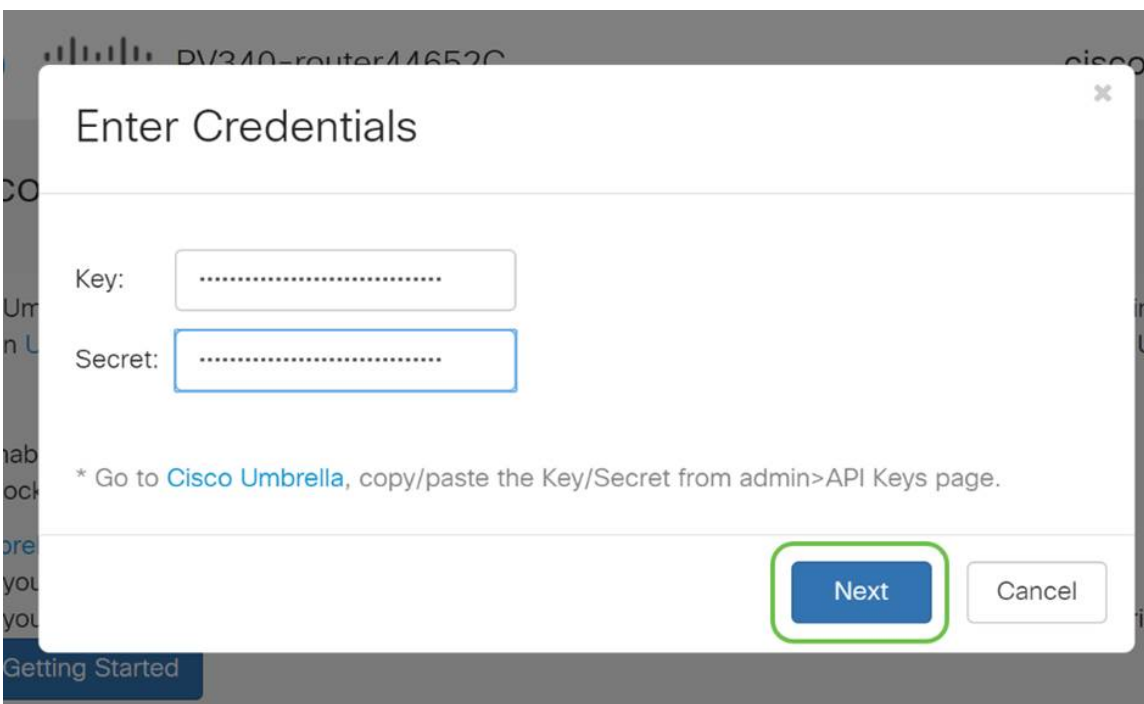
- If you use "Network" as this router's identity.
- If you use "Network Device" as this router's identity. (Preferred, if available in your Umbrella subscription)

Getting Started

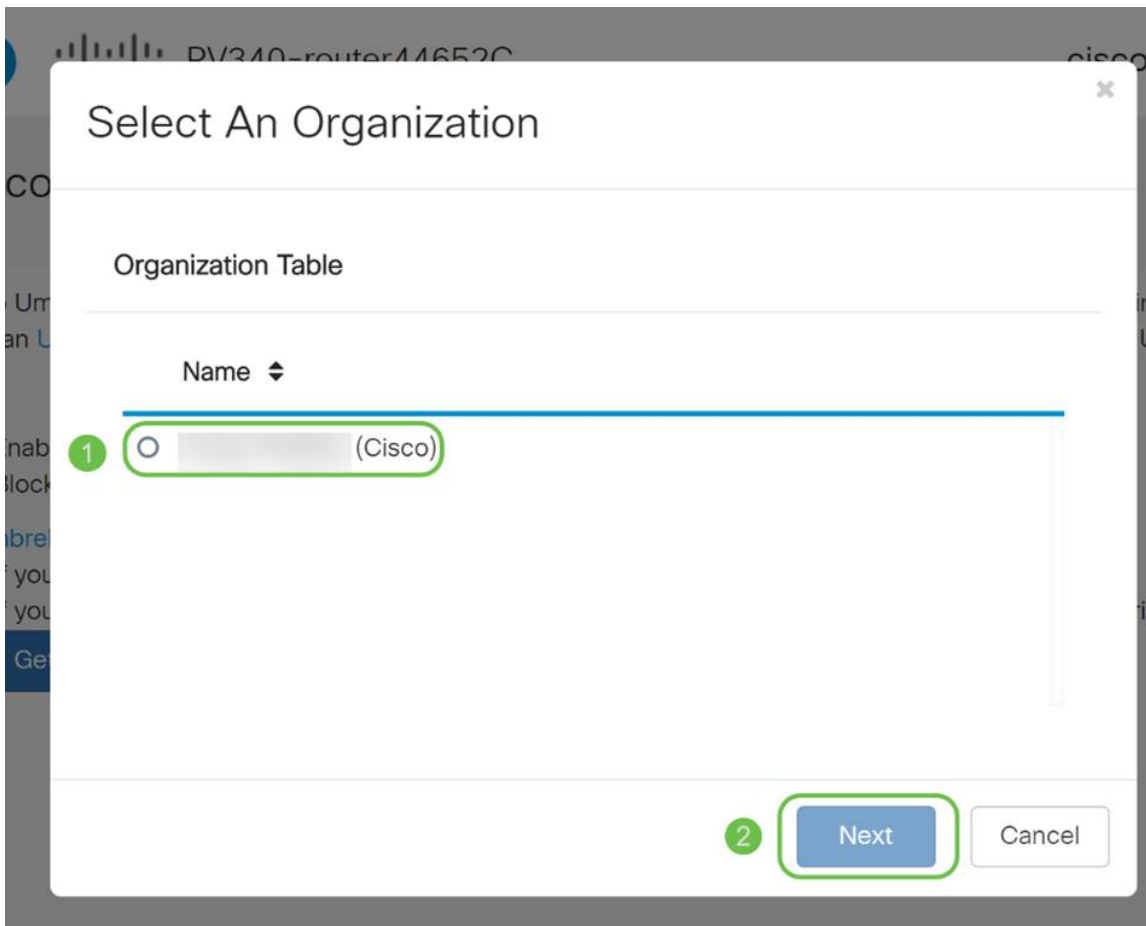
步骤6.现在在文本框中输入API Key和Secret Key。



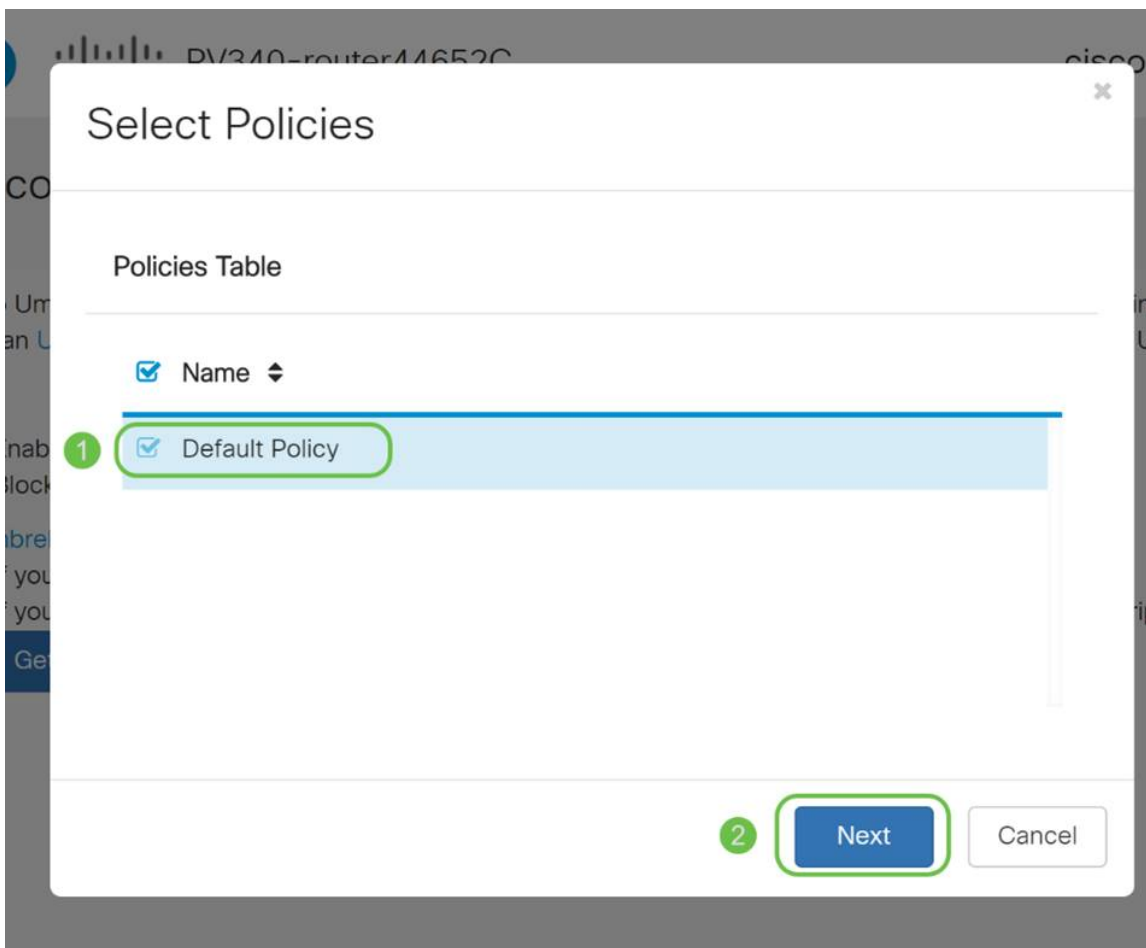
步骤7.输入API和密钥后，单击Next按钮。



步骤8.在下一个屏幕中，选择要与路由器关联的组织，然后单击下一步。

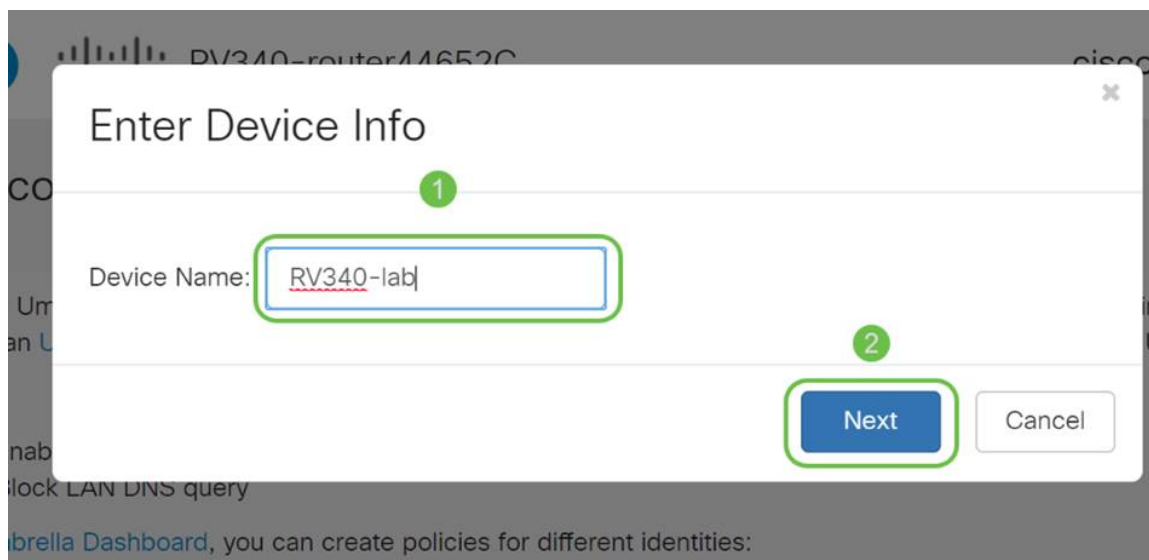


步骤9.现在选择要应用于RV34x路由的流量的策略。对于大多数用户，默认策略将提供足够的覆盖范围。

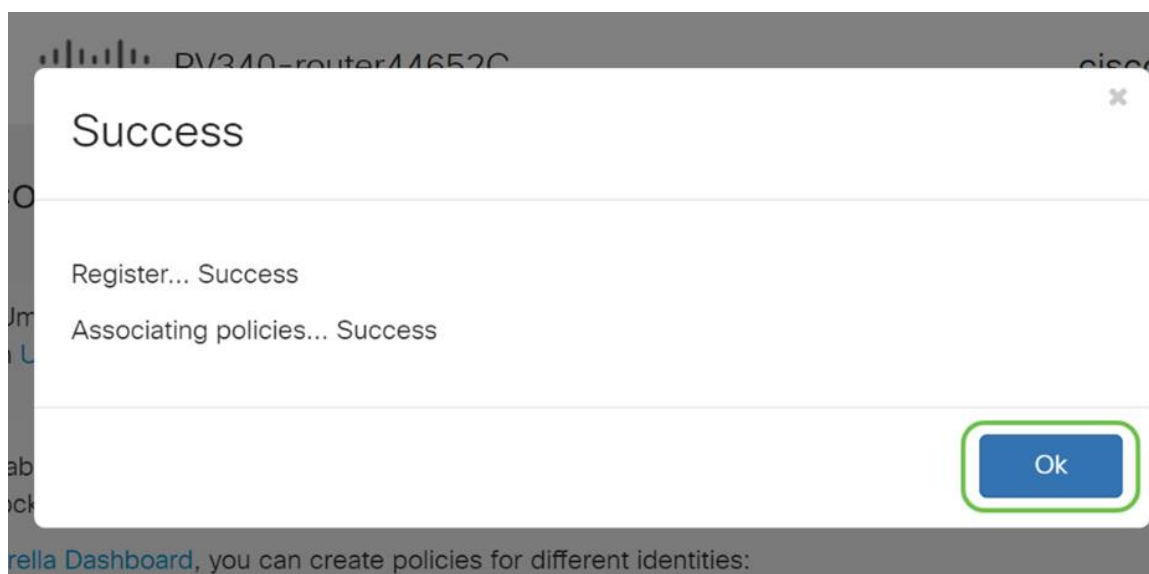


步骤10.为**设备指定**名称，以便可以在Umbrella报告中指定该设备。在我们的设置中，我们分

配了“RV340-lab”。



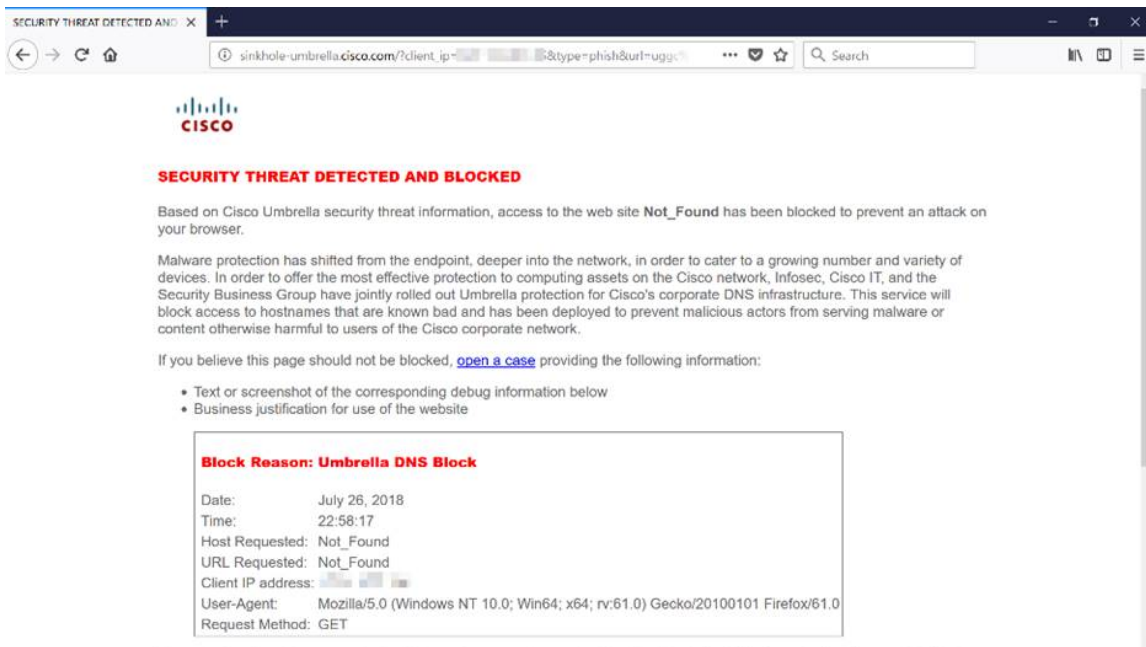
步骤11.成功关联后，下一个屏幕将验证所选设置并提供更新，然后点击**确定**。



确认一切都在正确的位置

祝贺您，您现在受到思科Umbrella的保护。还是你？我们通过一个实时示例反复检查，确保思科已创建了一个网站，该网站专用于在页面加载时快速确定问题。[单击此处](#)或在浏览器栏中键入<https://InternetBadGuys.com>。

如果Umbrella配置正确，您会看到类似此内容的屏幕！



查看与本文相关的视频.....

[单击此处查看思科的其他技术对话](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。