默认配置Web浏览器和HTTPS上的DNS

目录

简介

本文档介绍如何为Cisco Umbrella配置Web浏览器和HTTPS上的DNS默认设置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

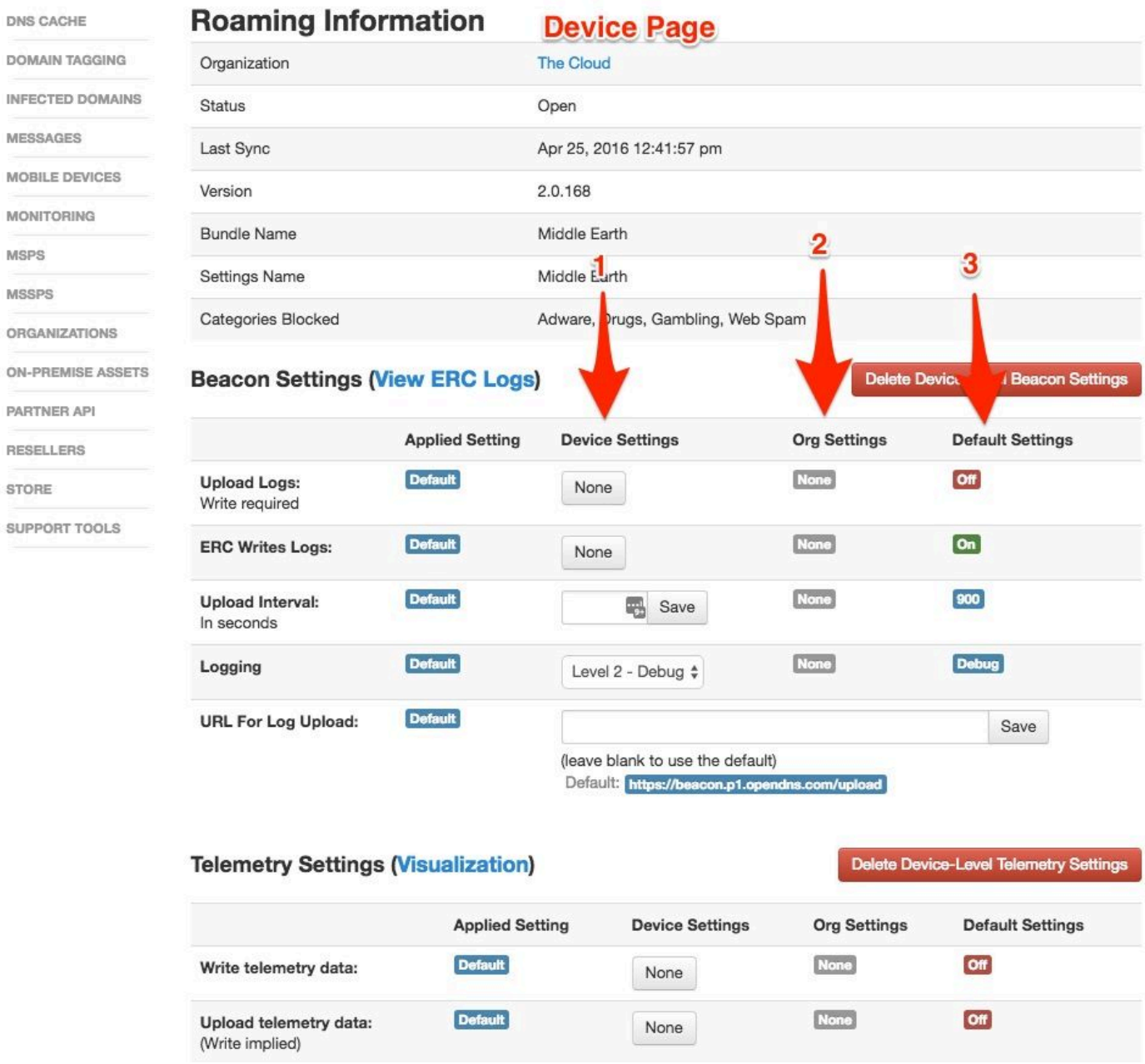
本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

从Firefox版本63开始，Mozilla可以为Firefox用户默认启用DNS-over-HTTPS(DoH)。这会将DoH发送到CloudFlare，CloudFlare可以绕过您的Umbrella设置。要保留您的Umbrella设置，请完成本文后面的步骤。

当Firefox启用DoH时，受影响的Firefox用户会看到此横幅：



1.jpg

在最新版本中，Chrome还将DoH作为手动配置提供。Chrome DoH只能在系统上存在的系统DNS服务器明确支持DoH时激活。因此，漫游客户端用户或本地DNS服务器网络不会看到启用了Chrome DoH。

使用Umbrella时默认为系统DNS

对于大多数Umbrella用户，此时无需任何操作。Firefox支持使用特殊域`use-application-dns.net`来表示DNS过滤解决方案（例如Cisco Umbrella）的存在。如果客户端正在使用Umbrella解析程序，则Firefox不会默认启用DoH。

但是，如果用户在Firefox中手动配置了DoH，Firefox会遵守该配置并使用定义的DoH服务器。在这种情况下，为了防止网络上的用户使用DoH，您需要完成本文后面的其他说明。

根据Chrome 83的版本："如果您当前的DNS提供商支持，Chrome将自动切换到DNS-over-

HTTPS”。

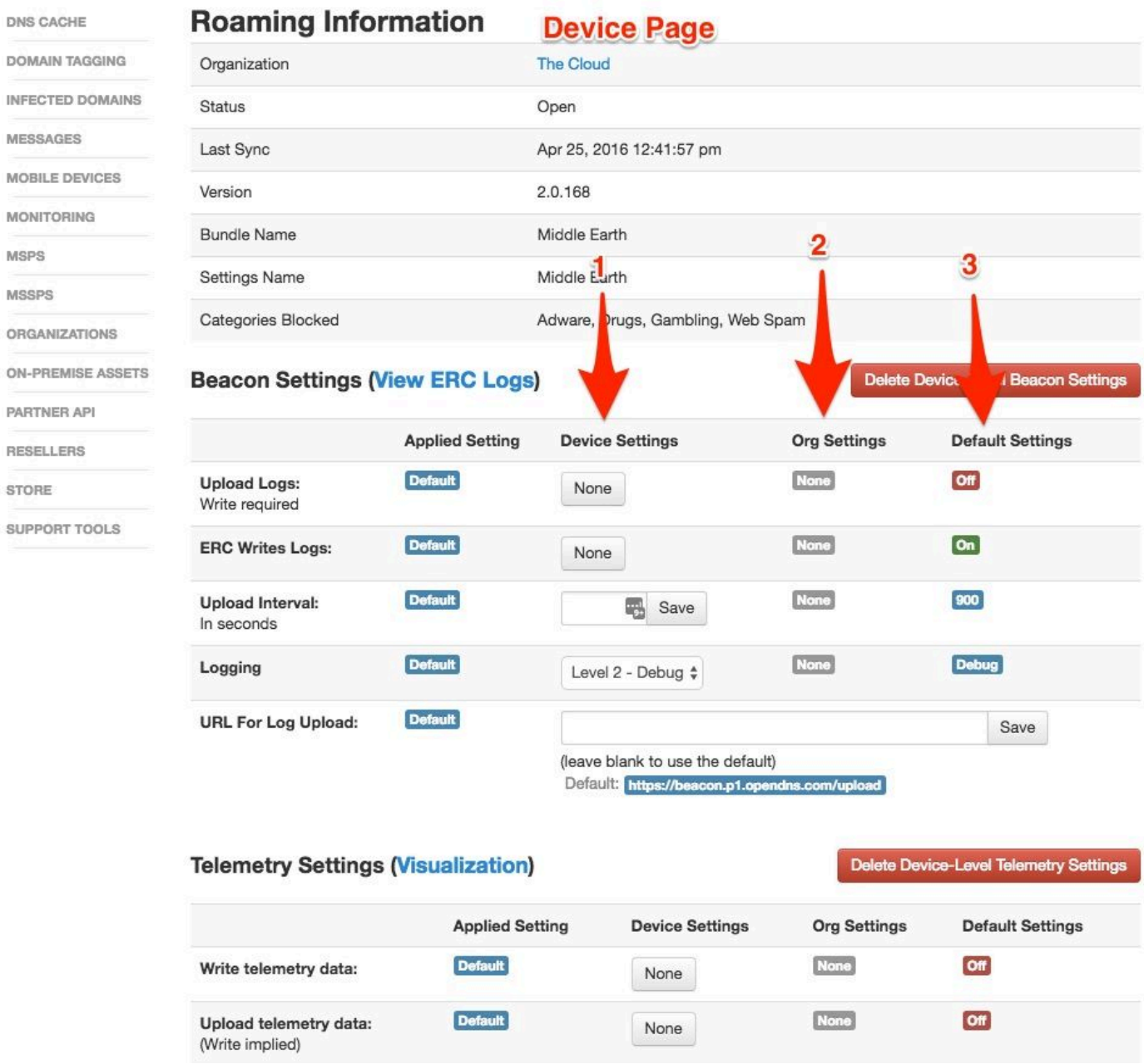
阻止基于HTTPS的DNS的其他说明

为了保护您的Umbrella部署，Umbrella现已将DoH提供商纳入到代理/匿名程序内容类别中。当此类别被阻止时，浏览器无法解析DoH服务器的主机名，并回复到Umbrella覆盖您的DNS的标准系统DNS。要确保设置阻止DoH提供程序：

1.定位至策略>内容类别。

2.选择正在使用的类别设置。

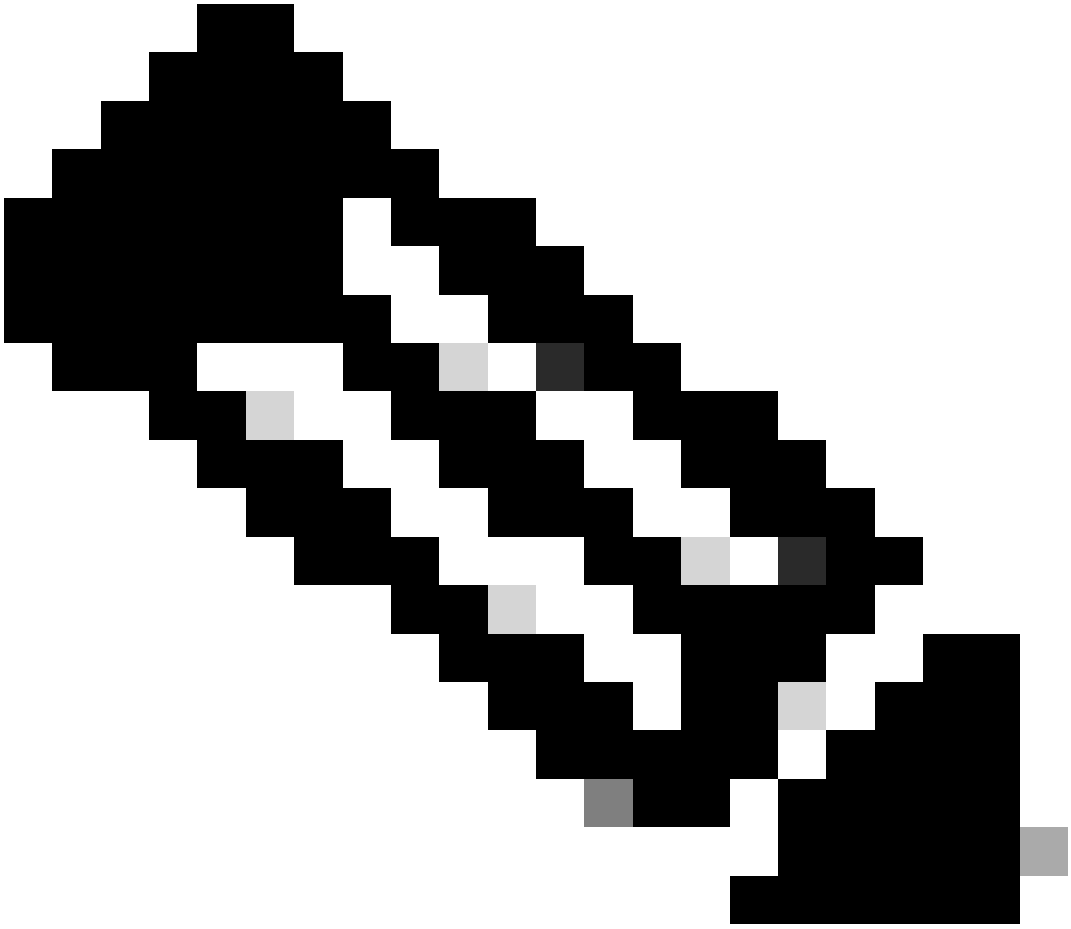
3.确保选中Proxy/Anonymizer。



1.jpg

4.保存更新。

现在，当Firefox向您的用户推出此更改时，您的用户仍可以继续由Umbrella覆盖。



> 注意：请勿将Mozilla Kill Switch域添加到阻止列表。这是因为，如果阻止了域，Umbrella会返回阻止页面的A记录。Firefox将此视为有效响应，因此可以自动升级其DoH。

其他建议

Firefox也可以为特定DoH提供程序手动配置。如果按域进行配置，则可由Umbrella强制执行。Umbrella(DNS)无法强制执行IP配置。 对于DoH的网络实施，可能需要防火墙规则。有关参考，请参阅通过防火墙规则防止规避Cisco Umbrella。

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）。