# 配置Umbrella VA以接收用户 — IP映射

## 目录


简介

先决条件

- 要求
- 使用的组件

概述

虚拟设备

- 向VA添加私钥和证书
- 向VA添加证书
- 在VA上启用HTTPS
- 验证HTTPS启用

Active Directory

Umbrella Android客户端

Umbrella Chromebook客户端

- 配置顺序


## 简介

本文档介绍如何配置Cisco Umbrella虚拟设备(VA)以通过安全通道接收用户 — IP映射。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

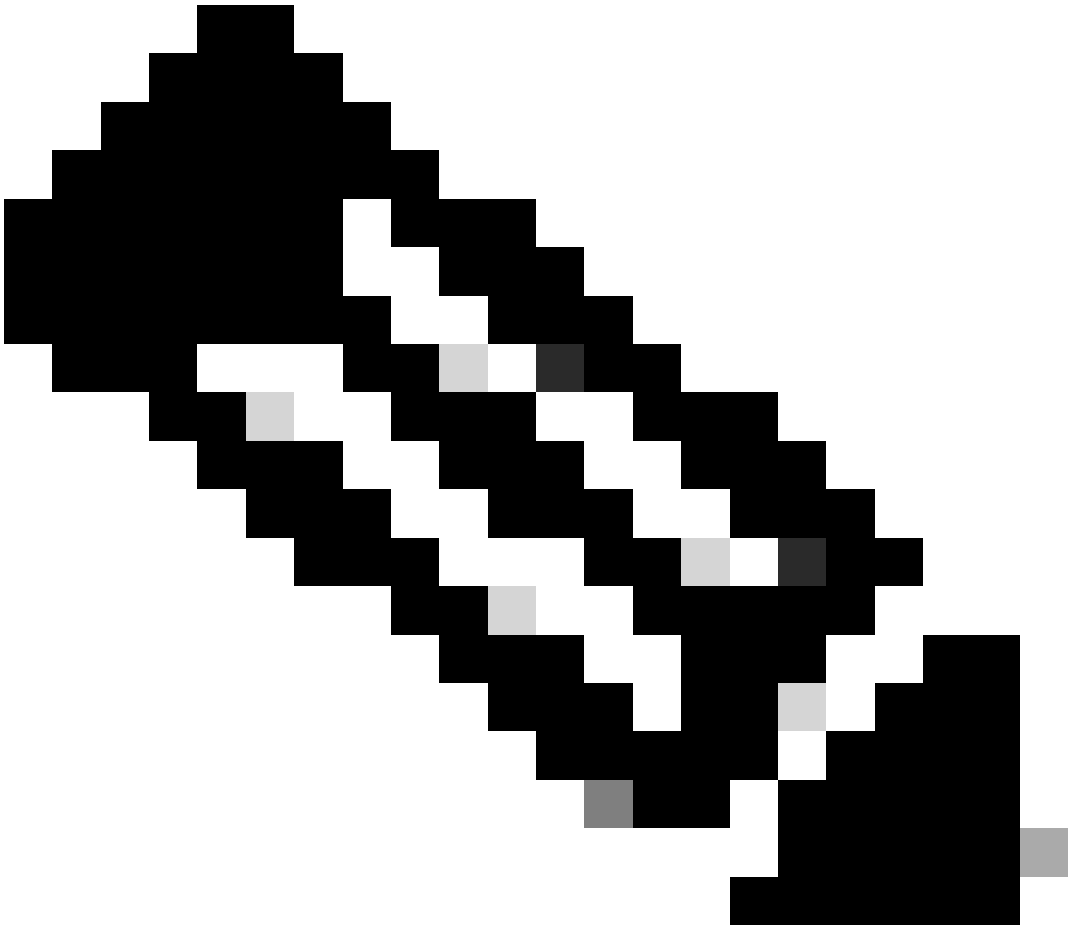
- 私钥创建、证书创建、证书签名和管理均不在Umbrella组件的范围内。这必须在这些组件的外部执行。
- 您必须为每个虚拟设备创建一个具有唯一公用名称的证书。
- 您还必须在内部DNS服务器中添加一个A记录，将此公用名指向虚拟设备的IP地址。
- 如果需要更改虚拟设备的IP地址，还必须相应地更改此A记录。
- 与证书对应的FQDN必须配置为Umbrella控制面板上的本地域，以便VA将其识别为本地域。
- 需要分别以.key和.cer格式创建私钥和证书。
- 为此，您可以使用自签名证书或CA签名证书。

## 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行版本2.7或更高版本的虚拟设备
- Umbrella AD连接器必须运行版本1.5或更高版本
- Umbrella Chromebook客户端必须运行版本1.3.3或更高版本

---



> 注意：如果您的VA或AD连接器运行的是以前的版本，您可以打开一个支持票证，以将其升级到相应的支持版本。

---

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。

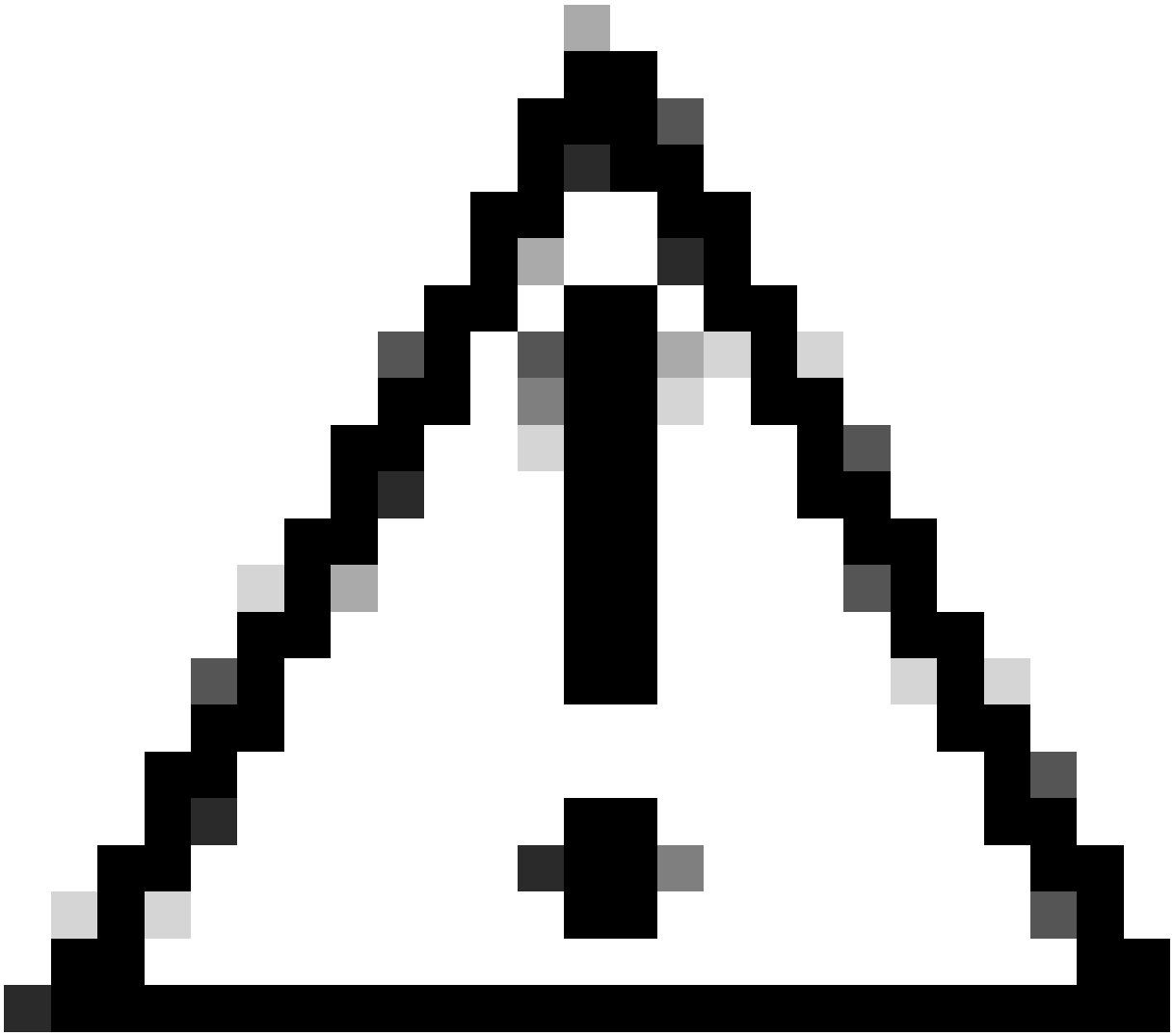
# 概述

运行版本2.6或更低版本的Umbrella虚拟设备支持在端口443上仅以未加密形式接收来自Umbrella Active Directory(AD)连接器和Umbrella Chromebook客户端的用户 — IP映射。因此，部署的一个必备条件是AD连接器和VA或Chromebook客户端和VA只能通过受信任网络通信。

从版本2.7开始，Umbrella虚拟设备现在可以通过HTTPS从AD连接器接收AD用户 — IP映射，同样也可以通过HTTPS从每个Umbrella Chromebook客户端接收GSuite用户 — IP映射。

本文详细介绍每个组件上启用HTTPS通信的配置步骤。默认情况下，HTTPS通信被禁用，AD连接器和Chromebook客户端仅通过HTTP与VA通信。

---



警告：启用此功能会增加VA和Umbrella AD连接器上的CPU和内存利用率，并会导致VA的DNS吞吐量降低。因此，建议仅在您的组织的任何合规性要求得到授权时启用此功能。

---

## 虚拟设备

### 向VA添加私钥和证书

将私钥和证书添加到VA的步骤：
1.通过文本编辑器打开私钥文件。

2.选择“全部”、“复制”，然后粘贴此命令的双引号：

```
config va ssl key "paste the contents of the .key file here"
```

## 向VA添加证书

将证书添加到VA的步骤：
1.通过文本编辑器打开证书文件。

2.选择“全部”、“复制”，然后粘贴以下命令的双引号：

```
config va ssl cert "paste the contents of the .crt file here"
```

## 在VA上启用HTTPS

使用以下命令在VA上启用HTTPS:

```
config va ssl enable
```

## 验证HTTPS启用

使用命令验证HTTPS是否已启用：

```
config va show
```

此命令的输出可包括HTTPS状态以及SSL证书详细信息。

示例输出：

```
HTTPS status : enabled
SSL Certificate Start Time : 2024-04-16 16:11:08
SSL Certificate Expiry Time : 2025-04-16 16:11:08
Issuer : C = US, ST = MASSACHUSETTS, L = BOSTON, O = CISCOSUPPORT, CN = server.domain.com
Common Names : vmhost.domain.com
```

VA最多可能需要20分钟才能开始通过HTTPS接收事件。大约20分钟后可以使用`config va status`命令进行检查。AD连接器状态在中间时段处于黄色（停止）状态，并且在VA开始通过HTTPS接收事件后变为绿色状态。

如果要禁用HTTPS并恢复为HTTP，请使用命令`config va ssl disable`。

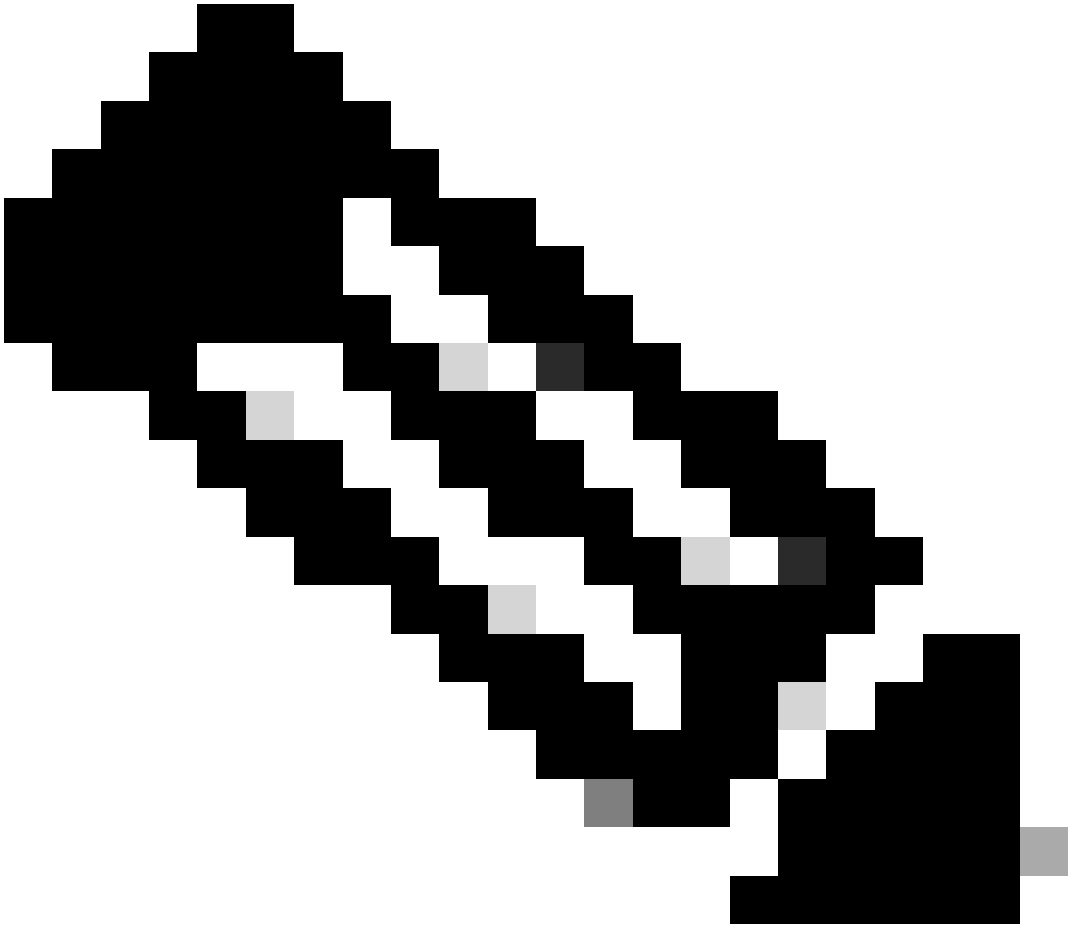
如果要重新启用HTTPS，必须再次添加私钥和证书，然后使用`config va enable`命令。

## Active Directory

如果为每个VA使用CA签名的证书，请确保在与VA位于同一站点中运行AD连接器的每个系统上安装根证书和为每个VA证书颁发CA证书。

如果您为每个VA使用自签名证书，请确保每个VA证书安装在与VA位于同一Umbrella站点中运行AD连接器的每个系统上。

---



---

注意：仅需要在AD连接器上安装与AD连接器位于同一Umbrella站点的VA证书。

VA最多可能需要20分钟才能将HTTPS状态同步到Umbrella，然后将其同步到AD连接器。因此，连接器开始通过HTTPS向VA发送数据可能需要20分钟。 VA会丢弃在此期间发送的任何用户 — IP映射。因此，建议仅在停机时间（预期用户不会登录时）对VA进行配置更改。

# Umbrella Android客户端

如果对VA使用CA签名证书，请确保将根证书和每个VA证书的颁发CA证书推送到每个Android设备并安装在设备上。

如果您对VA使用自签名证书，请确保每个VA证书被推送到每个Android设备上并安装。

证书可用后，Umbrella Android客户端可以开始使用此证书设置与VA的HTTPS通道。

# Umbrella Chromebook客户端

如果对VA使用CA签名证书，请确保将根证书和每个VA证书的颁发CA证书推送到每个Chromebook并安装在每个Chromebook上。

如果对VA使用自签名证书，请确保每个VA证书被推送到每个Chromebook并安装在每个Chromebook上。

证书可用后，Umbrella Chromebook客户端可以开始使用此证书设置与VA的HTTPS通道。

有关详细信息，请参阅文章Umbrella Chromebook Client:通过安全通道将用户 — IP映射发送到Umbrella虚拟设备。

## 配置顺序

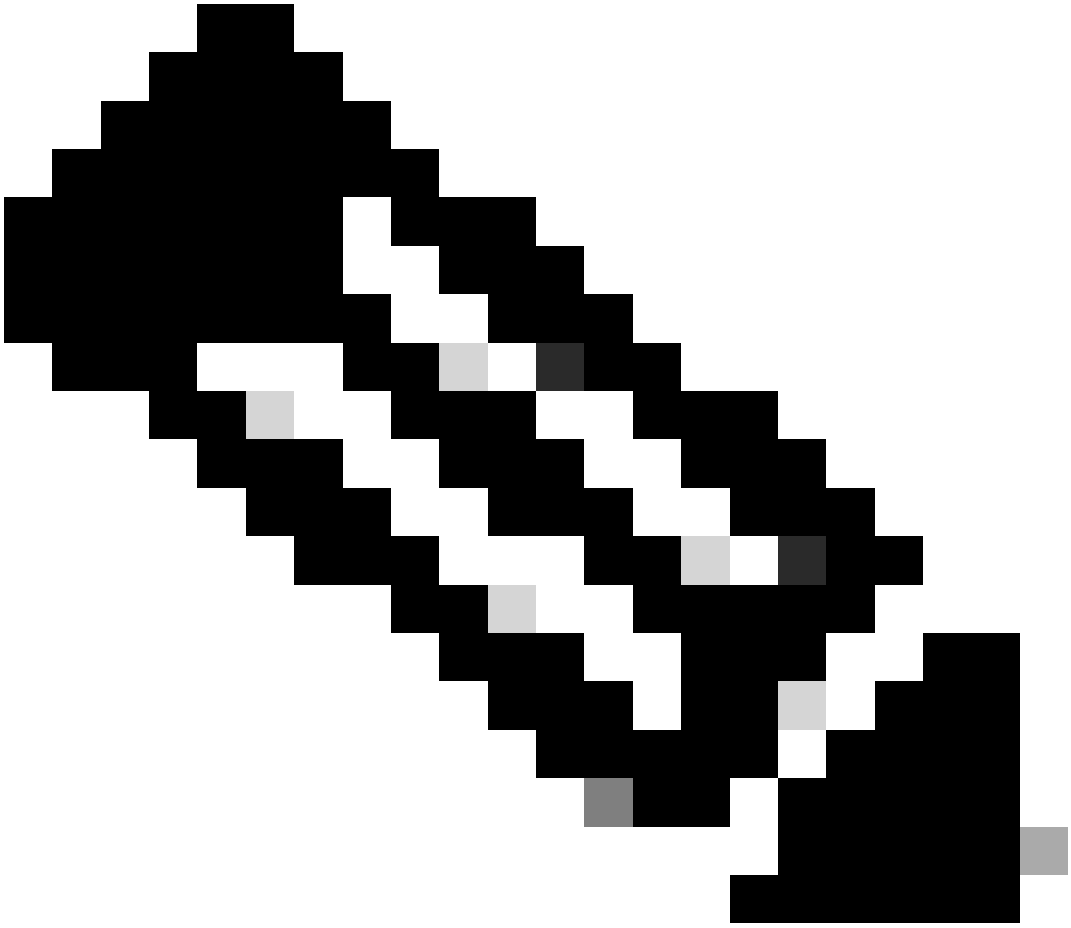
在VA上启用HTTPS后，VA不接受以明文形式通过HTTP发送的用户 — IP映射。因此，通过HTTP发送的任何用户登录都会被丢弃，并且这些用户的DNS请求的用户属性不可用。因此，建议按以下顺序配置这些组件：

1.根据CA签名或自签名证书为每个VA创建证书和私钥。

2.将证书和私钥分别添加到每个VA。

3.确保每个VA证书（或VA自签名证书）的根证书和中间父证书安装在与VA在同一站点中运行AD连接器的每个系统上以及每个Chromebook上。

4.在停机时间内，在VA上启用HTTPS。



注意：VA上的证书必须在到期之前替换，并且中间父级和根级证书必须安装在AD连接器和Umbrella Chromebook客户端上。如果不这样做，AD连接器和Umbrella Chromebook客户端将无法与VA通信。

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）。