

# 目录

[简介](#)

[证书概述](#)

[根证明](#)

[服务器证书](#)

[相关信息](#)

## 简介

本文描述应该使用在思科Web安全工具证书的种类(WSA)的HTTPS解密。

## 证书概述

WSA有能力使用一当前证书和专用密钥为了用在HTTPS解密上。然而，也许有关于应该使用证书的种类的混乱，因为不是所有的x.509证书工作。

有证书两种主要类型：**服务器证书**和**根证明**。所有x.509证书包含一个基本限制条件字段，识别证书种类：

- 附属的Type=End实体-服务器证书
- 附属的Type=CA -根证明

**注意：**必须使用根证明，也指Certificate Authority (CA)签署证书的您，在WSA的HTTPS解密。

## 根证明

根证明特别地创建为了签署服务器证书。您能创建和操作您自己的CA和签署您自己的服务器证书。

**注意：**因为根证明只签署其他证书，在Web服务器不可能用于为了进行HTTPS加密和解密。

WSA必须使用根证明为了积极地生成HTTPS解密的服务器证书。有两个选项可用为根证明使用情况：

- 生成在WSA的一个根证明。WSA创建其自己的根证明和专用密钥，并且使用此密钥对为了签署服务器证书。

- 您能上传一个当前根证明和其专用密钥到WSA。根证明的共同名称(CN)字段识别该的实体(典型地公司名称)信任包含其签名的所有服务器证书。

**注意：**在服务器证书可以是委托前，必须由有现在一个的公共密钥在Web浏览器的根证明签字。

## 服务器证书

服务器证书特别地创建为了用于HTTPS加密和解密和为了验证一个特定服务器的真实性。服务器证书由与使用的CA签字CA根证明。CA的一普通的示例是Verisign或Thawte。

**注意：**服务器证书不可能用于为了签署其他证书;因此，如果服务器证书在WSA，安装HTTPS解密不工作。

服务器证书的CN字段指定证书打算使用的主机。例如，<https://www.verisign.com>以www.verisign.com CN使用一服务器证书。

## 相关信息

- [Web安全工具\(WSA\)证书使用情况\(HTTPS解密、GUI登录，证件加密\)](#)
- [启用WSA &证书签名请求\(CSR\)选项的HTTPS代理的步骤](#)
- [启用HTTPS代理的步骤\(WSA\) &上传根/中间证书选项](#)
- [技术支持和文档 - Cisco Systems](#)