

在其他MDM平台上部署iOS版CSC

目录

[简介](#)

[背景信息](#)

[所有MDM](#)

[MobileIron云](#)

[Citrix终端管理MDM](#)

[Lightspeed MDM](#)

[JAMF学校](#)

[早于10.2.0的JAMF](#)

[InTune](#)

[莫希尔](#)

[安全](#)

简介

本文档介绍如何在其他移动设备管理平台上部署适用于iOS的思科安全连接器。

背景信息

iOS的[思科安全连接器\(CSC\)](#)是适用于iPhone的完整Umbrella DNS保护。在使用此指南进行部署之前，请阅读[CSC部署文档](#)。您的设备必须处于受控模式才能使用CSC。

本文档总结了CSC的其他移动设备管理(MDM)软件支持。这些MDM已通过成功的部署验证，但尚未直接显示在控制面板上。

要验证iOS设备上是否存在配置文件，请执行以下操作：

1. 导航到Settings > General > Device Management > [MDM Profile Name] > 更多详细信息。
2. 确认配置文件类型DNS Proxy与以下详细信息一起存在：
 - 应用详细信息：com.cisco.ciscosecurity.app
 - 提供商捆绑包详细信息：com.cisco.ciscosecurity.ciscoumbrella

[详细了解要在Apple MDM站点上配置哪些iOS配置文件。](#)

所有MDM

以下步骤适用于部署到所有MDM，必须首先完成：

1. 确保您的管理员电子邮件地址已添加到移动设备页面“设置”选项下的控制面板。
2. 下载Cisco_Umbrella_Root_CA.cer文件以在iOS设备上使用。此证书允许无错HTTPS阻止页面。
要获取根CA，请执行以下操作：

1. 导航到部署 > 配置 > 根证书。
2. 选择下载证书。
3. 将下载保存为 .cer 文件。

MobileIron云

目前，控制面板上的MobileIron下载仅支持内部版本。云版本使用的设备变量与现场软件不同。部署与内部部署非常相似，但也有一些例外。MobileIron核心可能需要此修改，具体视版本而定。

要部署到MobileIron云，请执行以下操作：

1. 确保您的管理员电子邮件地址已添加到移动设备页面“设置”选项下的控制面板。
2. 从Umbrella控制面板下载Mobile Iron配置文件。
3. 替换以下变量：

通用占位符变量	新变量
"\$DEVICE_SN\$"	\${deviceSN}
"\$DEVICE_MAC\$"*	\${deviceWifiMacAddress}

*仅用于CSC的Clarity组件，而不适用于Umbrella组件。如果不使用Clarity，则没有要替换的\$DEVICE_MAC\$。

Citrix终端管理MDM

要部署到Citrix，请在控制面板中完成以下准备步骤：

1. 确保您的管理员电子邮件地址已添加到移动设备页面“设置”选项下的控制面板。
2. 从Umbrella[下载通用MDM配置](#)（AMP以相同方式配置）。
3. 下载Umbrella的根证书：
 1. 导航到部署>配置>根证书。
 2. 选择下载证书。
 3. 将下载保存为 .cer 文件。
4. 修改配置并将通用占位符替换为[Citrix MDM的正确变量](#)：

通用占位符变量	新变量
序列号	\${device.serialnumber}
MAC_Address*	\${device.MAC_ADDRESS}

*仅用于CSC的Clarity组件，而不适用于Umbrella组件。

然后，完成以下MDM步骤：

- 1. 配置MDM以使用Apple Business Manager(ABM) (以前称为VPP，批量购买计划) 安装 CSC应用。
- 2. 上传准备步骤中修改的Umbrella和/或Clarity配置。
- 3. [使用Citrix文档中的步骤导入配置文件。](#)
- 4. 为设备上传证书以信任[Umbrella Root Certificate Authority](#)。
- 5. 配置策略以将配置文件、1个CA和1个CSC应用推送到所需的设备。

Lightspeed MDM

Lightspeed MDM支持iOS DNS代理的基于文本的配置。这可以通过修改通用MDM配置文件来实现。

- 1. 下载“generic mobileconfig file”并将文件扩展名从.xml更改为.txt。
- 2. 打开文件，将第58行上的占位符序列号字符串更改为%serial_number%
- 3. 在Lightspeed中，将思科安全连接添加到DNS代理配置文件，如下所示

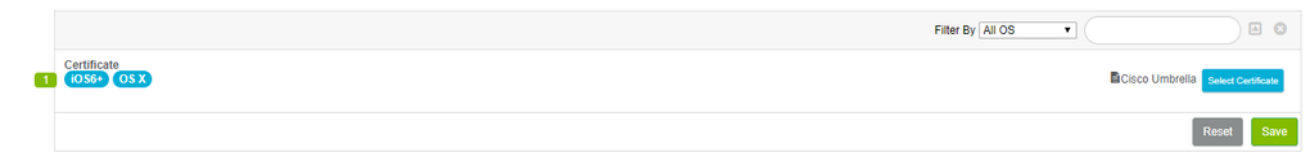


360019477192

- 4. 将修改的通用mobileconfig文件添加到应用下方的DNS代理配置选项。

360019477152

- 5. 最后，从Umbrella下载[Cisco Root CA](#)并将其部署在Lightspeed中，以确保阻止页面没有证书



360019477132

这些步骤适用于部署到所有MDM。请先执行这些步骤。

JAMF学校

使用JAMF Schools部署CSC与JAMF不同。从通用配置文件开始，并参见JAMF文档中的[步骤](#)。

以下是选择位置以及序列号使用变量的配置示例：

PayloadContent

AppBundleIdentifier

com.cisco.ciscosecurity.app

PayloadDescription

Cisco Umbrella

PayloadDisplayName

Cisco Umbrella

PayloadIdentifier

com.apple.dnsProxy.managed.{pre-filled in the download}

PayloadType

com.apple.dnsProxy.managed

PayloadUUID

{pre-filled in the download}

PayloadVersion

1

ProviderBundleIdentifier

com.cisco.ciscosecurity.app.CiscoUmbrella

ProviderConfiguration

disabled

disabled

internalDomains

10.in-addr.arpa

16.172.in-addr.arpa

17.172.in-addr.arpa

18.172.in-addr.arpa

19.172.in-addr.arpa

20.172.in-addr.arpa

21.172.in-addr.arpa

22.172.in-addr.arpa

23.172.in-addr.arpa

24.172.in-addr.arpa

25.172.in-addr.arpa

26.172.in-addr.arpa

27.172.in-addr.arpa

28.172.in-addr.arpa

29.172.in-addr.arpa

30.172.in-addr.arpa

31.172.in-addr.arpa

168.192.in-addr.arpa

local

logLevel

verbose

orgAdminAddress

{pre-filled in the download}

organizationId

{pre-filled in the download}

regToken

{pre-filled in the download}

serialNumber

%SerialNumber%

PayloadDisplayName

Cisco Security

PayloadIdentifier

com.cisco.ciscosecurity.app.CiscoUmbrella.{pre-filled in the download}

PayloadRemovalDisallowed

PayloadType

Configuration

PayloadUUID

{pre-filled in the download}

PayloadVersion

1

1. 在JAMF学校创建新配置文件。
有关详细信息，请参阅[设备配置文件上的JAMF文档](#)。
2. 使用DNS代理负载配置以下设置：
 1. 在App Bundle ID字段中，输入com.cisco.ciscosecurity.app。
 2. 在Provider Bundle ID字段中，输入com.cisco.ciscosecurity.app.CiscoUmbrella。
3. 将您在JAMF文档的第2步中创建的XML文件[件添加](#)到提供商配置中。

早于10.2.0的JAMF

使用JAMF部署CSC需要大量修改配置文件。使用以下步骤部署带JAMF MDM的CSC。

1. 确保您的管理员电子邮件地址已添加到Mobile Devices页面Settings选项下的控制面板。
2. 添加Umbrella根CA：
 1. 导航到部署>配置>根证书。
 2. 选择Download Certificate。
 3. 将下载保存为.cer文件。
 4. 提供证书名称，然后选择上传证书。

5. 上传.cer并将密码字段留空。
6. 应用到设备范围以推出此证书。
3. 从Umbrella控制面板下载通用配置文件。
4. 如果您使用的是JAMF Pro v.10.2.0或更高版本，则可以跳过此步骤。您可以通过添加以下内容按原样导入：

```
<key>serialNumber</key>
<string>$SERIALNUMBER</string>
<key>label</key>
<string>$DEVICENAME</string>
```

5. 如果您使用的是低于v.10.2.0的JAMF版本，请广泛编辑XML配置文件，如本示例配置文件所示。请勿复制此示例，此示例未按原样工作。仅使用控制面板中的通用下载配置。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>AppBundleIdentifier</key>
<string>com.cisco.ciscosecurity.app</string>
<key>PayloadDescription</key>
<string>Cisco Umbrella</string>
<key>PayloadDisplayName</key>
<string>Cisco Umbrella</string>
<key>PayloadIdentifier</key>
<string>com.apple.dnsProxy.managed.DB2A157-E134-3E8C-B4FB-23EDF48A0CD1</string>
<key>PayloadType</key>
<string>com.apple.dnsProxy.managed</string>
<key>PayloadUUID</key>
<string>59401AAF-CDBF-4FD7-9250-443A58EAD706</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>ProviderBundleIdentifier</key>
<string>com.cisco.ciscosecurity.app.CiscoUmbrella</string>
<key>ProviderConfiguration</key>
<dict>
<key>disabled</key>
<false/>
<key>internalDomains</key>
<array>
<string>10.in-addr.arpa</string>
<string>16.172.in-addr.arpa</string>
<string>17.172.in-addr.arpa</string>
<string>18.172.in-addr.arpa</string>
<string>19.172.in-addr.arpa</string>
<string>20.172.in-addr.arpa</string>
<string>21.172.in-addr.arpa</string>
<string>22.172.in-addr.arpa</string>
<string>23.172.in-addr.arpa</string>
<string>24.172.in-addr.arpa</string>
<string>25.172.in-addr.arpa</string>
<string>26.172.in-addr.arpa</string>
<string>27.172.in-addr.arpa</string>
```

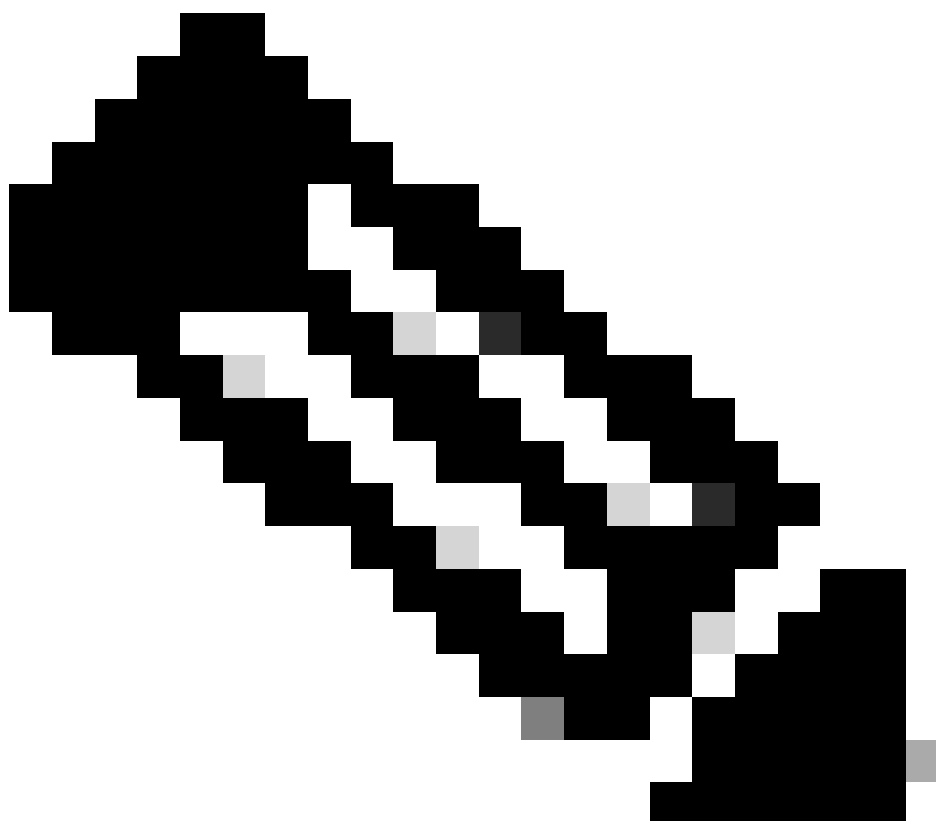
```

<string>28.172.in-addr.arpa</string>
<string>29.172.in-addr.arpa</string>
<string>30.172.in-addr.arpa</string>
<string>31.172.in-addr.arpa</string>
<string>168.192.in-addr.arpa</string>
<string>local</string>
<string>cisco.com</string>
</array>
<key>logLevel</key>
<string>{pre-filled in the download}</string>
<key>orgAdminAddress</key>
<string>{pre-filled in the download}</string>
<key>organizationId</key>
<string>{pre-filled in the download}</string>
<key>regToken</key>
<string>{pre-filled in the download}</string>
<key>serialNumber</key>
<string>$SERIALNUMBER</string>
<key>label</key>
<string>$DEVICENAME</string>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>Cisco Security</string>
<key>PayloadIdentifier</key>
<string>com.cisco.ciscosecurity.app.CiscoUmbrella.{pre-filled in the download}</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>{pre-filled in the download}</string>
<key>PayloadVersion</key>
<integer>{pre-filled in the download}</integer>
</dict>
</plist>

```

6. 导入到JAMF:

1. 在MDM主配置窗口下，单击New创建新配置文件。



注意：此配置文件必须是单独的配置文件，不能与创建的证书配置文件一起使用。要使应用正常工作，必须将这两个配置文件单独推送到设备。

-
2. 命名配置文件并导航到DNS代理。
 3. 在DNS代理下，单击Configure。
 4. 将代理配置设置为Umbrella详细信息：
 1. 在App Bundle ID字段中，输入`com.cisco.ciscosecurity.app`。
 2. 在Provider Bundle ID字段中，输入`com.cisco.ciscosecurity.app.CiscoUmbrella`。
 3. 从Umbrella粘贴编辑的XML内容到提供商配置中XML部分。
 5. 单击Scope并应用到正确的设备范围。

InTune

InTune会直接添加到Umbrella控制面板。有关详细信息，请参阅[Umbrella InTune文档](#)。



注意：Clarity是面向终端的思科AMP的产品。如果您当前未获得此产品的许可，请跳过相关的设置部分。

莫希尔

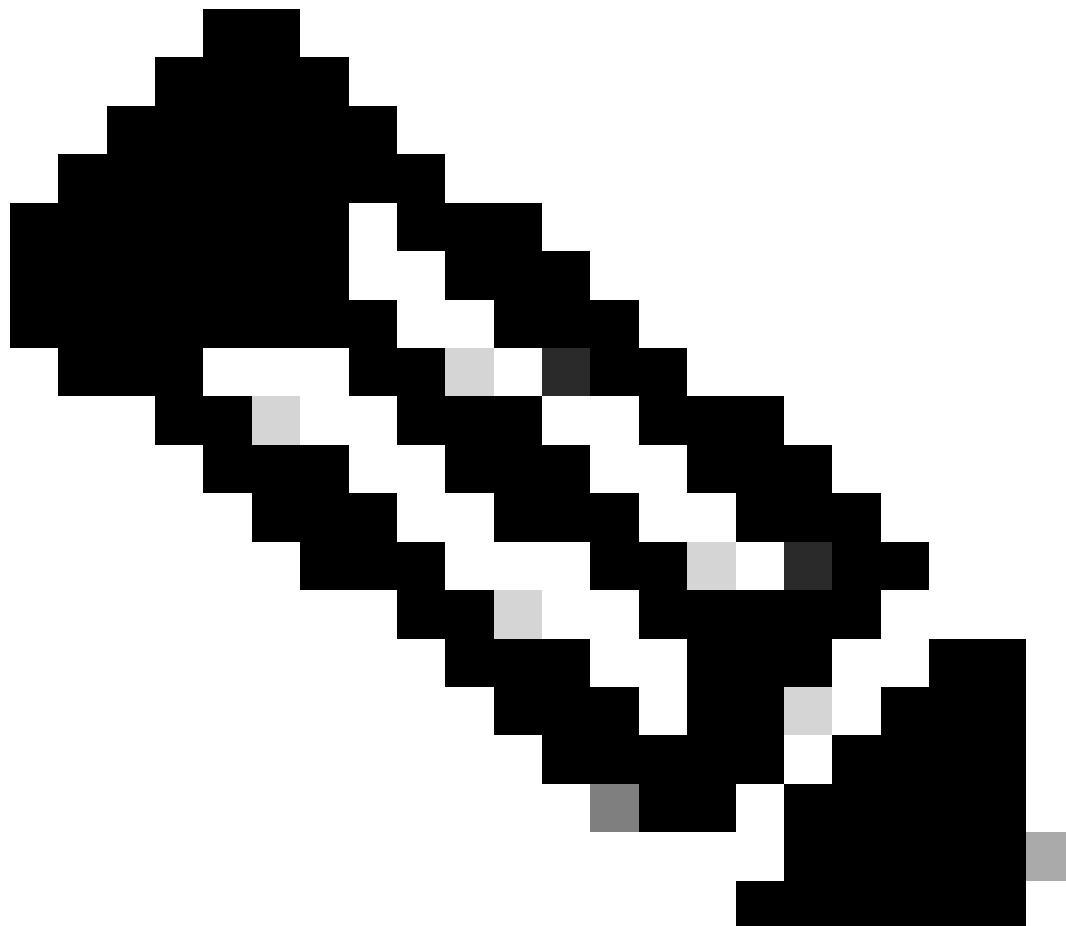
Mosyle支持采用DNS代理配置的形式：

- 在App Bundle ID字段中，输入`com.cisco.ciscosecurity.app`。
- 在Provider Bundle ID字段中，输入`com.cisco.ciscosecurity.app.CiscoUmbrella`。

将XML<key>ProviderConfiguration</key>中的内容添加到Module Provider Configuration字段中：

```
<dict>
<key>anonymizationLevel</key>
<integer>0</integer>
```

```
***  
<key>serialNumber</key>  
<string>%SerialNumber%</string>  
</dict>
```



注意：这些设置要求为设备设定作用域以接收配置，默认情况下不会添加作用域。

安全

在DNS代理配置文件页面上配置安全：

- 在应用捆绑包ID字段中，输入com.cisco.ciscosecurity.app
- 在Provider Bundle ID字段中，输入com.cisco.ciscosecurity.app.CiscoUmbrella

使用以下步骤配置.plist文件：

1. 从iOS Common Config模板开始，将文件编辑为.plist，在

<key>ProviderConfiguration</key>注释中仅包含<dict>到</dict>。

2. 将serialNumber密钥替换为\$serialnumber变量（如Securly所定义）。

3. .plist文件内容可能与此示例非常相似。将此项上传到DNS代理配置：

anonymizationLevel

0

disabled

internalDomains

10.in-addr.arpa

16.172.in-addr.arpa

17.172.in-addr.arpa

18.172.in-addr.arpa

19.172.in-addr.arpa

20.172.in-addr.arpa

21.172.in-addr.arpa

22.172.in-addr.arpa

23.172.in-addr.arpa

24.172.in-addr.arpa

25.172.in-addr.arpa

26.172.in-addr.arpa

27.172.in-addr.arpa

28.172.in-addr.arpa

29.172.in-addr.arpa

30.172.in-addr.arpa

31.172.in-addr.arpa

168.192.in-addr.arpa

local

LogLevel

{pre-filled in the download}

orgAdminAddress

{pre-filled in the download}

organizationId

{pre-filled in the download}

regToken

{pre-filled in the download}

serialNumber

\$serialnumber

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）。