

在其他MDM平台上部署CSC for iOS

目錄

[簡介](#)

[背景資訊](#)

[所有MDM](#)

[MobileIron雲端](#)

[Citrix端點管理MDM](#)

[Lightspeed MDM](#)

[JAMF學校](#)

[低於10.2.0的JAMF](#)

[InTune](#)

[莫希爾](#)

[安全](#)

簡介

本文說明如何在其他流動裝置管理平台上部署適用於iOS的思科安全聯結器。

背景資訊

適用於iOS的 [思科安全聯結器\(CSC\)](#) 是適用於iPhone的完整Umbrella DNS保護。在將此指南用於部署之前，請閱讀[CSC部署文檔](#)。您的裝置必須處於受監控模式才能使用CSC。

本檔案將總結適用於CSC的其他流動裝置管理(MDM)軟體支援。這些MDM已通過成功的部署驗證，但尚未直接顯示在控制面板上。

要驗證iOS裝置上是否存在配置檔案，請執行以下操作：

1. 導航至Settings > General > Device Management > [MDM Profile Name] > More details。
2. 確認檔案型別DNS Proxy是否存在，以及以下詳細資訊：
 - 應用詳細資訊：com.cisco.ciscosecurity.app
 - 提供商捆綁包詳細資訊：com.cisco.ciscosecurity.ciscoumbrella

[詳細瞭解要在Apple MDM站點上配置的iOS配置檔案詳細資訊。](#)

所有MDM

以下步驟適用於部署到所有MDM，必須首先完成：

1. 確保將您的管理員電子郵件地址新增到Mobile Devices頁面「Settings」選項下的控制面板中。
2. 下載Cisco_Umbrella_Root_CA.cer檔案，以在iOS裝置上使用。此憑證允許使用無錯誤HTTPS封

鎖頁面。要獲取根CA，請執行以下操作：

1. 導覽至Deployments > Configuration > Root Certificate。
2. 選擇Download Certificate。
3. 將下載內容另存為.cer檔案。

MobileIron雲端

目前，儀表板上的MobileIron下載僅支援內部版本。雲版本使用的裝置變數與現場軟體不同。部署與現場部署非常相似，但存在一些例外。MobileIron核心可能需要此修改，具體取決於版本。

要部署到MobileIron雲，請執行以下操作：

1. 確保將您的管理員電子郵件地址新增到Mobile Devices頁面「Settings」選項下的控制面板中。
2. 從Umbrella控制面板下載Mobile Iron配置檔案。
3. 替換以下變數：

通用佔位符變數	新變數
"\$DEVICE_SN\$"	\${deviceSN}
"\$DEVICE_MAC\$"*	\${deviceWifiMacAddress}

*這僅用於CSC的Clarity元件，而不用於Umbrella元件。如果不使用Clarity，則沒有要替換的\$DEVICE_MAC\$。

Citrix端點管理MDM

要部署到Citrix，請在儀表板中完成以下準備步驟：

1. 確保將您的管理員電子郵件地址新增到Mobile Devices頁面「Settings」選項下的控制面板中。
2. 從Umbrella[下載通用MDM配置](#)（AMP以相同方式配置）。
3. 下載Umbrella的根證書：
 1. 導覽至Deployments > Configuration > Root Certificate。
 2. 選擇Download Certificate。
 3. 將下載內容另存為.cer檔案。
4. 修改配置並將通用佔位符替換為[Citrix MDM](#)的正確變數：

通用佔位符變數	新變數
序列號	\${device.serialnumber}

MAC地址*	\${device.MAC_ADDRESS}
--------	------------------------

*這僅用於CSC的Clarity元件，而不用於Umbrella元件。

然後，完成以下MDM步驟：

1. 配置MDM以使用Apple Business Manager(ABM) (以前稱為VPP，批次購買程式) 安裝CSC應用。
2. 上傳在準備步驟中修改的Umbrella和/或Clarity配置。
3. [使用Citrix文檔中的步驟匯入配置檔案。](#)
4. 上傳裝置的證書以信任[Umbrella Root Certificate Authority](#)。
5. 配置策略以將配置檔案、1個CA和1個CSC應用推送到所需的裝置。

Lightspeed MDM

Lightspeed MDM支援iOS DNS代理的基於文本的配置。這可以通過修改通用MDM配置檔案來實現。

1. 下載「通用mobileconfig檔案」並將副檔名從.xml更改為.txt。
2. 開啟檔案，將第58行上的佔位符序列號字串更改為%serial_number%
3. 在Lightspeed中，將思科安全連線新增到DNS代理配置檔案，如下所示



360019477192

4. 將修改後的通用mobileconfig檔案新增到應用下面的DNS代理配置選項中。

360019477152

5. 最後，從Umbrella下載[思科根CA](#)，並將其部署在Lightspeed中，以確保無證書阻止頁面。

360019477132

這些步驟適用於部署到所有MDM。請首先使用這些步驟。

JAMF學校

使用JAMF Schools部署CSC與JAMF不同。從通用配置檔案開始，請參閱[JAMF文檔](#)中的步驟。

以下是選擇何處和將哪個變數用於序列號的配置示例：

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學校建立新配置檔案。
有關詳細資訊，請參閱[裝置配置檔案上的JAMF文檔](#)。
2. 使用DNS代理負載配置以下設定：
 1. 在「App Bundle ID」欄位中，輸入com.cisco.ciscosecurity.app。
 2. 在「Provider Bundle ID」欄位中，輸入com.cisco.ciscosecurity.app.CiscoUmbrella。
3. 將您在JAMF文檔步驟2中建立的XML檔案[新增到](#)Provider Configuration中。

低於10.2.0的JAMF

使用JAMF部署CSC需要大量修改配置檔案。使用以下步驟使用JAMF MDM部署CSC。

1. 確保將您的管理員電子郵件地址新增到Mobile Devices頁面Settings選項下的儀表板中。
2. 新增Umbrella根CA：
 1. 導覽至Deployments > Configuration > Root Certificate。
 2. 選擇Download Certificate。

3. 將下載內容另存為.cer檔案。
 4. 提供證書名稱，然後選擇Upload Certificate。
 5. 上傳.cer並將密碼欄位留空。
 6. 應用於裝置範圍以推出此證書。
3. 從Umbrella控制面板下載通用配置檔案。
4. 如果您使用的是JAMF Pro v.10.2.0或更高版本，則可以跳過此步驟。您可以通過新增以下內容按原樣匯入：

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

5. 如果您使用的是低於v.10.2.0的JAMF版本，請按照本示例配置檔案中的說明詳細編輯XML配置檔案。請勿複製此示例，該示例無法按原樣工作。僅使用儀表板中的通用下載配置。

```
<?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>
```

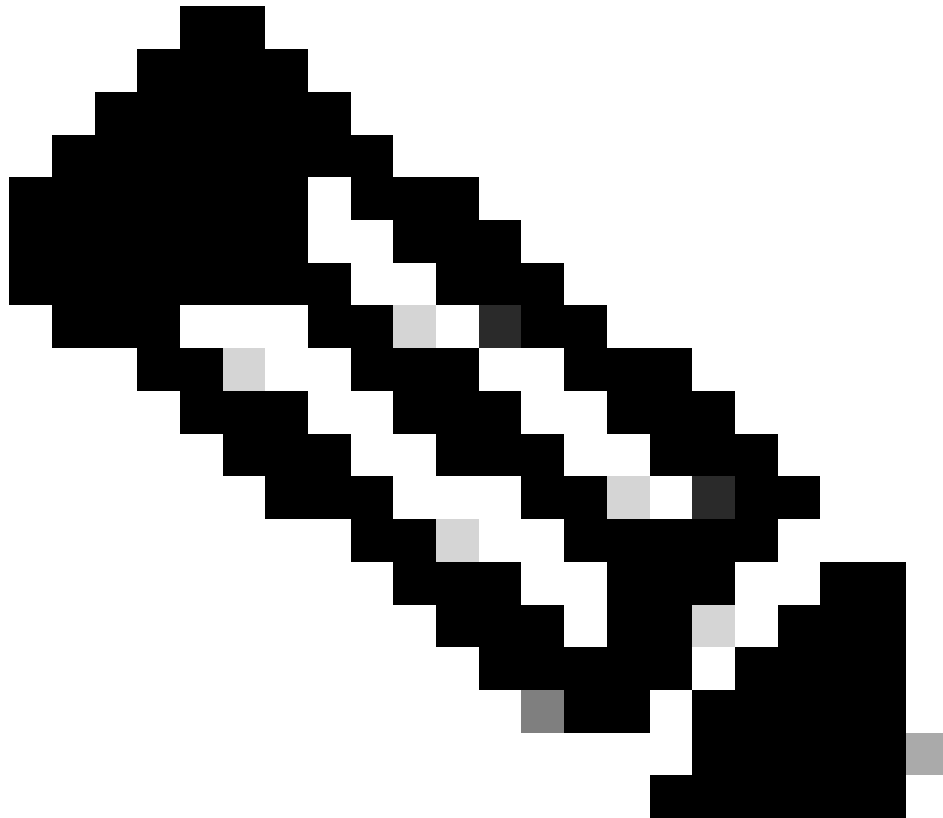
```

<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. 匯入到JAMF:

1. 在MDM主配置視窗下，按一下New建立新配置檔案。

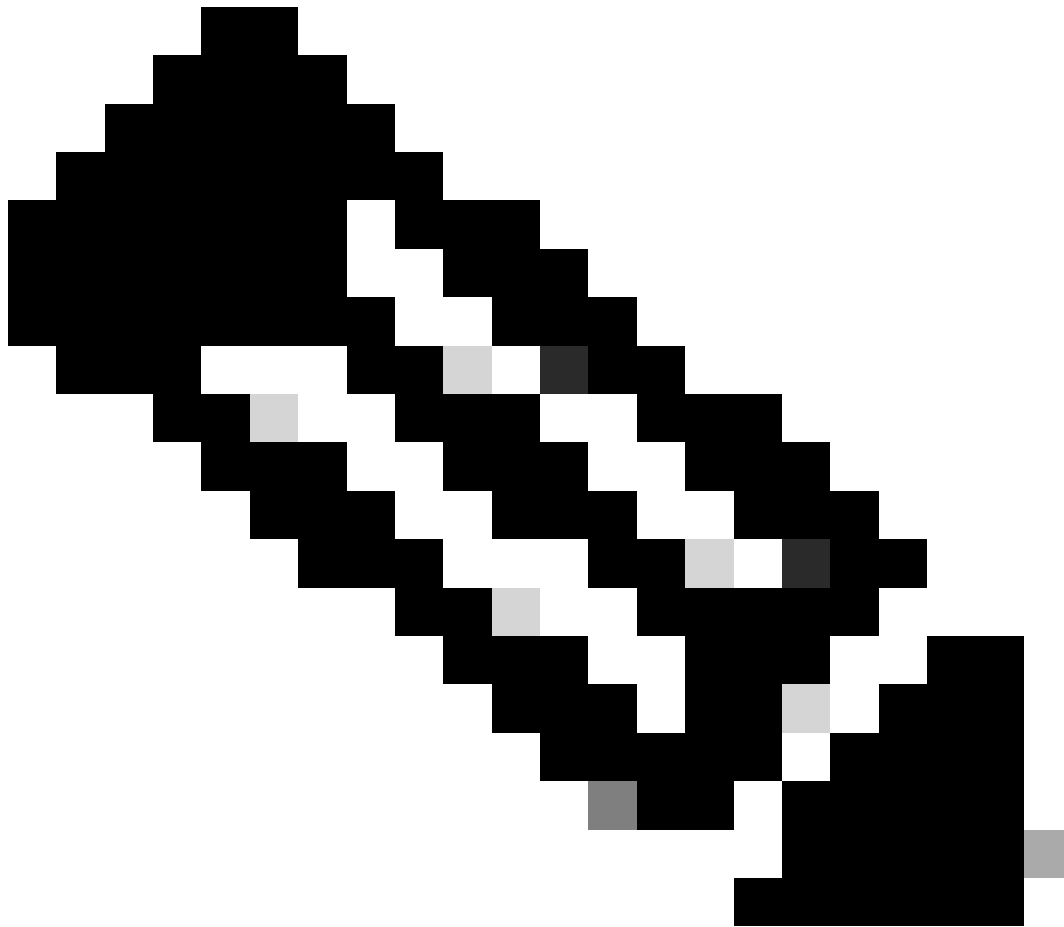


附註：此配置檔案必須是單獨的配置檔案，不能與建立的證書配置檔案一起使用。要使應用正常工作，必須分別將這兩個配置檔案推送到裝置。

-
2. 命名配置檔案並導航到DNS代理。
 3. 在DNS代理下，按一下Configure。
 4. 將代理配置設定為Umbrella詳細資訊：
 1. 在「App Bundle ID」欄位中，輸入`com.cisco.ciscosecurity.app`。
 2. 在「Provider Bundle ID」欄位中，輸入`com.cisco.ciscosecurity.app.CiscoUmbrella`。
 3. 從Umbrella貼上編輯的XML內容到提供程式配置XML部分。
 5. 按一下Scope並應用到正確的裝置範圍。

InTune

InTune將直接新增到Umbrella控制面板。有關更多資訊，請檢視[Umbrella InTune文檔](#)。



附註：Clarity是面向終端的思科AMP的產品。如果您目前尚未獲得此產品的許可，請跳過相關的設定部分。

莫希爾

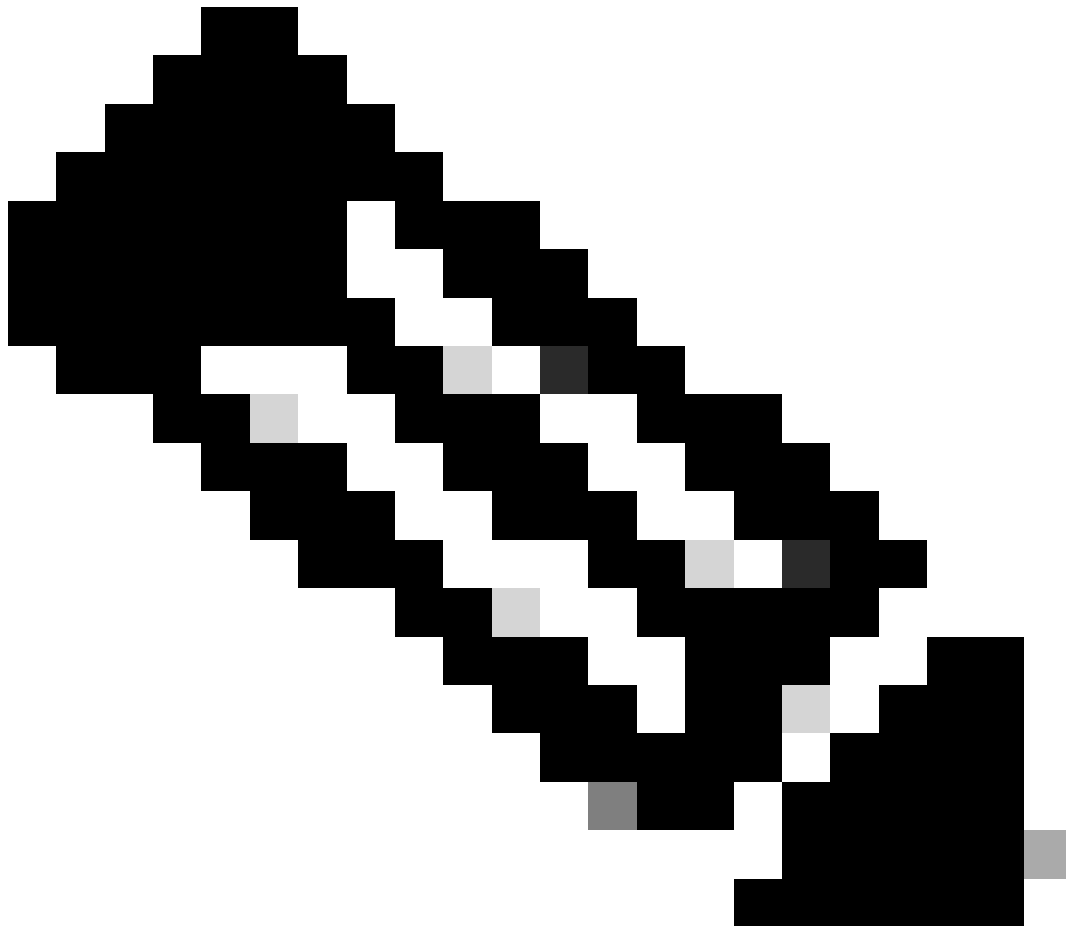
DNS代理配置的形式支援模組：

- 在「App Bundle ID」欄位中，輸入`com.cisco.ciscosecurity.app`。
- 在「Provider Bundle ID」欄位中，輸入`com.cisco.ciscosecurity.app.CiscoUmbrella`。

將XML<key>ProviderConfiguration</key>中的內容新增到Module Provider Configuration欄位中：

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

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



附註：這些設定要求為裝置設定作用域以接收配置，預設情況下不新增作用域。

安全

在DNS代理配置檔案頁面上配置安全：

- 在「App Bundle ID」欄位中，輸入com.cisco.ciscosecurity.app
- 在「Provider Bundle ID」欄位中，輸入com.cisco.ciscosecurity.app.CiscoUmbrella

使用以下步驟配置.plist檔案：

1. 從iOS通用配置模板開始，將檔案編輯到.plist，其中僅包含<dict>到

</dict><key>ProviderConfiguration</key>註釋中的<dict>到</dict>。

2. 將serialNumber鍵替換為\$serialnumber變數 (如Securly所定義) 。

3. .plist檔案內容可能與本示例非常相似。將此上傳到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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。