# Implementación de CSC para iOS en plataformas de MDM adicionales

## Contenido



## Introducción

Este documento describe cómo implementar Cisco Security Connector para iOS en plataformas de administración de dispositivos móviles adicionales.

## Antecedentes

Cisco Security Connector (CSC) para iOS ofrece una protección completa de Umbrella DNS para su iPhone. Antes de utilizar esta guía para implementaciones, lea la documentación de implementación de CSC. El dispositivo debe estar en el modo supervisado para utilizar el CSC.

Este documento resume la compatibilidad adicional del software de gestión de dispositivos móviles (MDM) para el CSC. Una implementación correcta ha validado estos MDM, pero todavía no están presentes directamente en el panel.

Para verificar que existe un perfil en un dispositivo con iOS:

1. Vaya a Settings > General > Device Management > [MDM Profile Name] > More details.
2. Confirme que el tipo de perfil DNS Proxy esté presente junto con estos detalles:
    - Detalles de la aplicación: `com.cisco.ciscosecurity.app`
    - Detalles del paquete del proveedor: `com.cisco.ciscosecurity.ciscoumbrella`

Más información sobre los detalles del perfil de iOS que se configurarán en el sitio de MDM de Apple.

# Todos los MDM

Estos pasos se aplican para la implementación en todos los MDM y se deben completar primero:

1. Asegúrese de que la dirección de correo electrónico del administrador se agrega al panel en la opción "Configuración" de la página Dispositivos móviles.
2. Descargue el archivo `Cisco_Umbrella_Root_CA.cer` para utilizarlo en el dispositivo con iOS. Este certificado permite páginas de bloque HTTPS sin errores. Para obtener la CA raíz:
    1. Vaya a Implementaciones > Configuración > Certificado raíz.
    2. Seleccione Descargar certificado.
    3. Guarde la descarga como un archivo `.cer`.

# Nube de MobileIron

Actualmente, la descarga de MobileIron en el panel solo admite la versión en las instalaciones. La versión en nube utiliza variables de dispositivo diferentes a las del software en las instalaciones. La implementación es muy similar a la in situ, con varias excepciones. MobileIron Core en función de la versión puede requerir esta modificación.

Para realizar la implementación en MobileIron Cloud:

1. Asegúrese de que la dirección de correo electrónico del administrador se agrega al panel en la opción "Configuración" de la página Dispositivos móviles.
2. Descargue el perfil de Mobile Iron desde el panel de Umbrella.
3. Reemplace estas variables:

| Variable de marcador de posición genérico | Nueva variable |
|---|---|
| `"$DEVICE_SN$"` | `${deviceSN}` |
| `"$DEVICE_MAC$"`* | `${deviceWifiMacAddress}` |

*Solo se utiliza para el componente Clarity del CSC, no para el componente Umbrella. Si no utiliza Clarity, no hay $DEVICE_MAC$ que sustituir.

# MDM de Citrix Endpoint Management

Para realizar la implementación en Citrix, siga estos pasos de preparación en el panel:

1. Asegúrese de que la dirección de correo electrónico del administrador se agrega al panel en la opción "Configuración" de la página Dispositivos móviles.
2. Descargue la configuración genérica de MDM de Umbrella (AMP se configura del mismo modo).

3. Descargue el certificado raíz para Umbrella:
    1. Vaya a Implementaciones > Configuración > Certificado raíz.
    2. Seleccione Descargar certificado.
    3. Guarde la descarga como un archivo `.cer`.
4. Modifique la configuración y sustituya el marcador de posición genérico por la variable correcta para Citrix MDM:

| Variable de marcador de posición genérico | Nueva variable |
|---|---|
| `serial_number` | `${device.serialnumber}` |
| `Dirección_MAC*` | `${device.MAC_ADDRESS}` |

*Solo se utiliza para el componente Clarity del CSC, no para el componente Umbrella.

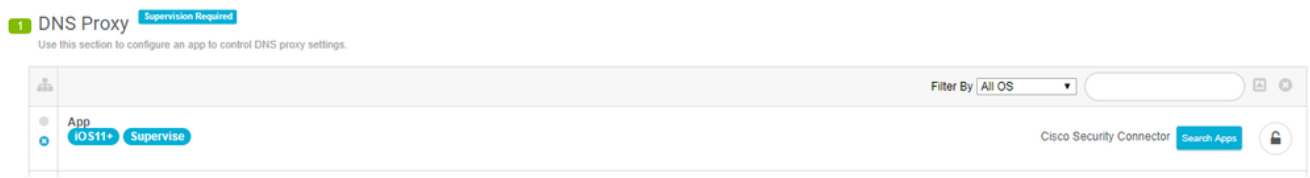
A continuación, complete estos pasos de MDM:

1. Configure MDM para instalar la aplicación CSC mediante Apple Business Manager (ABM) (anteriormente conocido como VPP, Volume Purchase Program).
2. Cargue la configuración de Umbrella y/o Clarity modificada en los pasos de preparación.
3. Siga los pasos de la documentación de Citrix para importar el perfil.
4. Cargue el certificado para que el dispositivo confíe en la Autoridad de certificados raíz de Umbrella.
5. Configure las políticas para enviar los perfiles, 1 CA y 1 aplicación CSC a los dispositivos requeridos.

## MDM de velocidad ligera

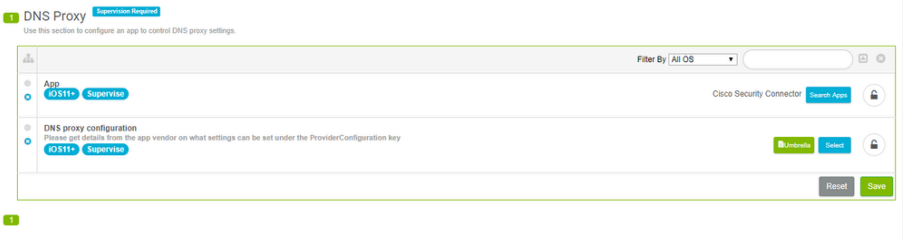
Lightspeed MDM soporta la configuración basada en texto del proxy DNS de iOS. Esto se puede lograr modificando el perfil genérico de MDM.

1. Descargue el "archivo mobileconfig genérico" y cambie la extensión del archivo de .xml a .txt.
2. Abra el archivo y cambie la cadena del número de serie del marcador de posición en la línea 58 a `%serial_number%`
3. En Lightspeed, agregue la conexión de seguridad de Cisco al perfil de proxy DNS como se muestra




360019477192

4. Agregue el archivo mobileconfig genérico modificado a la opción de configuración de proxy DNS debajo de la aplicación.




360019477152

5. Por último, descargue la CA raíz de Cisco de Umbrella e impleméntelo en Lightspeed para asegurarse de que las páginas de bloques no tengan certificados.

360019477132

Estos pasos se aplican a la implementación en todos los MDM. Siga estos pasos en primer lugar.

## Escuelas de JAMF

La implementación de CSC con JAMF Schools difiere de JAMF. Comience con el perfil genérico y vea los pasos en la documentación de JAMF.

A continuación se muestra un ejemplo de configuración de dónde seleccionar y qué variable utilizar para el número de serie:

```
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. Cree un nuevo perfil en JAMF School.
   Para obtener más información, consulte la documentación de JAMF sobre perfiles de dispositivo.
2. Utilice la carga del proxy DNS para configurar estos parámetros:
   1. En el campo App Bundle ID, introduzca `com.cisco.ciscosecurity.app`.
   2. En el campo Provider Bundle ID, introduzca `com.cisco.ciscosecurity.app.CiscoUmbrella`.
3. Agregue el archivo XML que creó en el paso 2 de la documentación de JAMF a la Configuración del proveedor.

## JAMF anterior a 10.2.0

La implementación de CSC con JAMF requiere una modificación significativa del perfil. Siga estos pasos para implementar el CSC con JAMF MDM.

1. Asegúrese de que la dirección de correo electrónico del administrador se agrega al panel en la opción Configuración de la página Dispositivos móviles.
2. Agregue la CA raíz de Umbrella:
   1. Vaya a Implementaciones > Configuración > Certificado raíz.
   2. Seleccione Descargar certificado.
   3. Guarde la descarga como un archivo .cer.
   4. Proporcione un nombre para el certificado y seleccione Cargar certificado.
   5. Cargue el archivo .cer y deje el campo de contraseña en blanco.
   6. Aplique al alcance de sus dispositivos para extender este certificado.
3. Descargue el perfil genérico desde el panel de Umbrella.
4. Si utiliza JAMF Pro v.10.2.0 o superior, puede omitir este paso. Puede importar tal cual agregando lo siguiente:

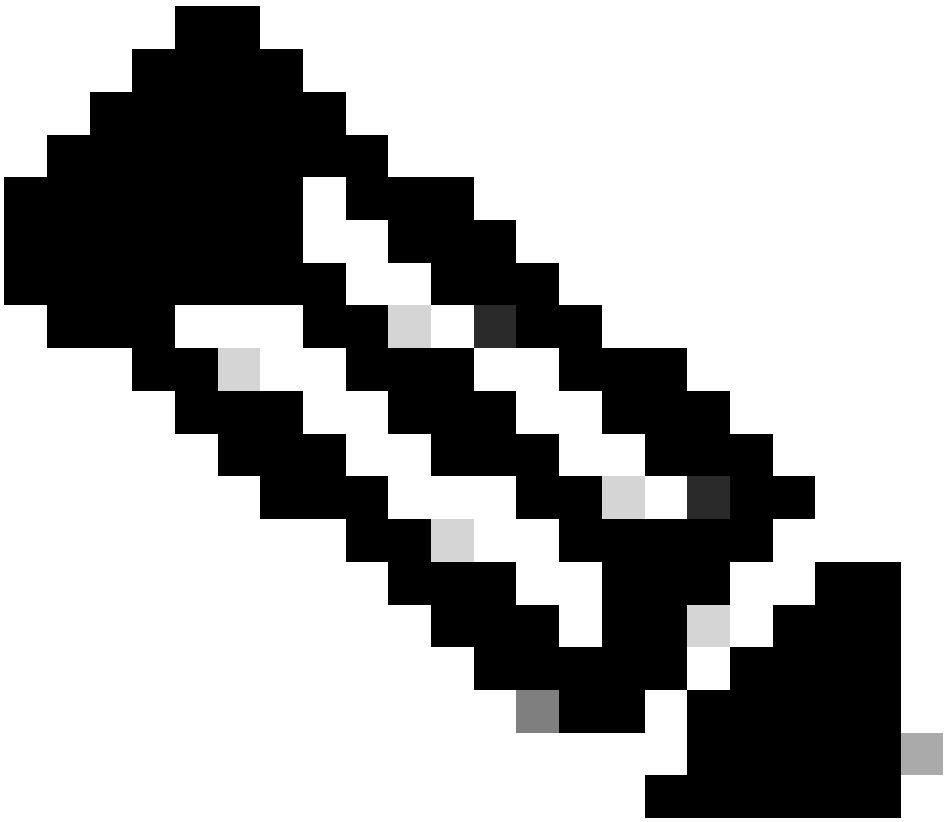
   ```
   <key>serialNumber</key>
   <string>$SERIALNUMBER</string>
   <key>label</key>
   <string>$DEVICENAME</string>
   ```

5. Si utiliza una versión de JAMF anterior a la v.10.2.0, edite el perfil XML de forma exhaustiva, como se muestra en este perfil de ejemplo. No copie este ejemplo, ya que no funciona tal cual. Utilice únicamente la configuración de descarga genérica del panel.

<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.d
<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.DBE2A157-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. Importar a JAMF:
    1. En la ventana principal de configuración de MDM, haga clic en New para crear un nuevo perfil.



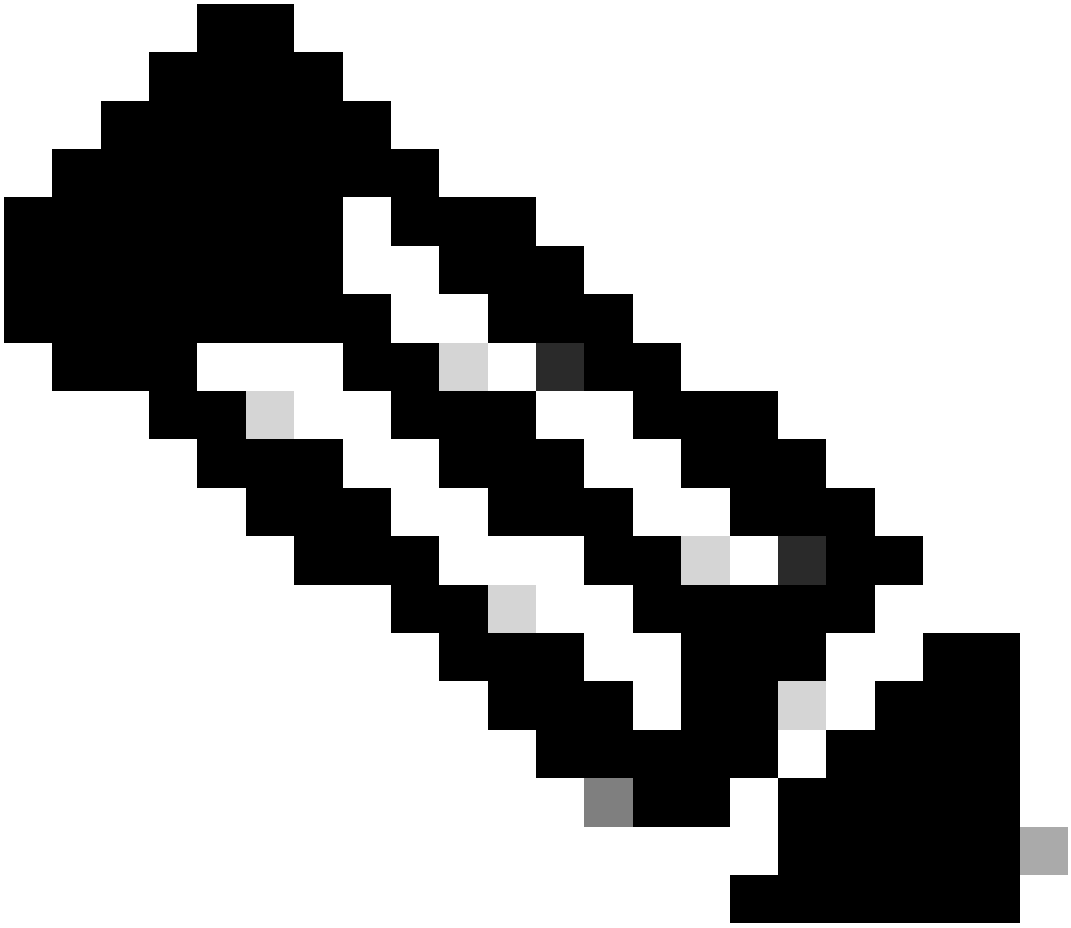
Nota: Debe ser un perfil independiente y no debe utilizarse con el perfil de certificado creado. Para que la aplicación funcione, estos dos perfiles deben

enviarse al dispositivo por separado.

2. Asigne un nombre al perfil y desplácese hasta Proxy DNS.
3. En el proxy DNS, haga clic en Configurar.
4. Establezca la configuración de proxy en Detalles de Umbrella:
    1. En el campo App Bundle ID, introduzca `com.cisco.ciscosecurity.app`.
    2. En el campo Provider Bundle ID, introduzca `com.cisco.ciscosecurity.app.CiscoUmbrella`.
    3. Pegar el contenido XML editado desde Umbrella en la configuración del proveedor sección XML.
5. Haga clic en Ámbito y aplique al ámbito adecuado de los dispositivos.

## InTune

InTune se agrega directamente al panel de Umbrella. Consulte la documentación de Umbrella InTune para obtener más información.



Nota: Clarity es un producto de Cisco AMP para terminales. Si actualmente no dispone de una licencia para este producto, omita la parte de configuración relacionada.

## Mosela

El soporte de Mosyle se encuentra en la forma de la configuración de proxy DNS:

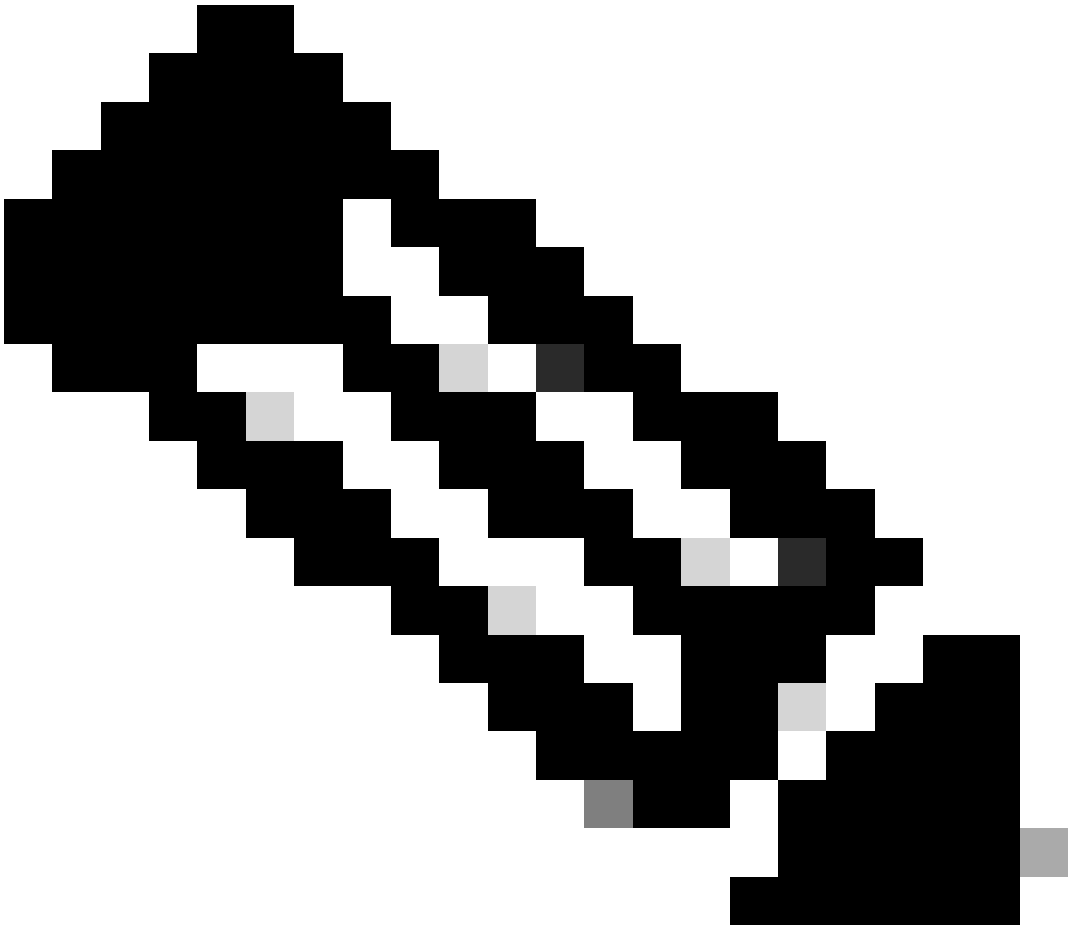
- En el campo App Bundle ID, introduzca `com.cisco.ciscosecurity.app`.
- En el campo Provider Bundle ID, introduzca `com.cisco.ciscosecurity.app.CiscoUmbrella`.

Agregue el contenido dentro de XML `<key>ProviderConfiguration</key>` al campo Configuración del Proveedor de Móviles:

```
<dict>
```

```
<key>anonymizationLevel</key>
<integer>0</integer>
***
<key>serialNumber</key>
<string>%SerialNumber%</string>
</dict>
```

---



> Nota: La configuración requiere que los dispositivos tengan un ámbito para recibir la configuración y los ámbitos no se agregan de forma predeterminada.

---

## Seguridad

Configurar de forma segura en la página Perfil de proxy DNS:

- En el campo App Bundle ID, introduzca `com.cisco.ciscosecurity.app`
- En el campo Provider Bundle ID, introduzca `com.cisco.ciscosecurity.app.CiscoUmbrella`

Utilice estos pasos para configurar el archivo `.plist`:

1. Comience con la plantilla de configuración común de iOS y edite el archivo en una `.plist` con solo los comentarios `<dict>` a través de `</dict>` dentro de `<key>ProviderConfiguration</key>`.
2. Reemplace la clave `serialNumber` con la variable `$serialnumber` tal como la define Securly.
3. El contenido del archivo `.plist` puede tener un aspecto muy similar a este ejemplo. Cargue esto en la configuración de proxy DNS:

```
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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).