Bereitstellung von CSC für iOS auf zusätzlichen MDM-Plattformen

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Cisco Security Connector für iOS auf zusätzlichen Managementplattformen für Mobilgeräte bereitgestellt wird.

Hintergrundinformationen

Der Cisco Security Connector (CSC) für iOS bietet umfassenden Umbrella DNS-Schutz für Ihr iPhone. Bevor Sie dieses Handbuch für Bereitstellungen verwenden, lesen Sie bitte die CSC-Bereitstellungsdokumentation. Das Gerät muss sich im überwachten Modus befinden, um den CSC verwenden zu können.

In diesem Dokument wird die zusätzliche MDM-Software (Mobile Device Management) für das CSC zusammengefasst. Diese MDMs wurden durch eine erfolgreiche Bereitstellung validiert, sind jedoch noch nicht direkt im Dashboard vorhanden.

So überprüfen Sie, ob auf einem iOS-Gerät ein Profil vorhanden ist:

1. Navigieren Sie zu Einstellungen > Allgemein > Gerätemanagement > [MDM-Profilname] > Weitere Details.
2. Vergewissern Sie sich, dass der Profiltyp DNS-Proxy mit folgenden Details vorhanden ist:
    - App-Details: `com.cisco.ciscosecurity.app`
    - Details zum Anbieterpaket: `com.cisco.ciscosecurity.ciscoumbrella`

Erfahren Sie mehr darüber, welche iOS-Profildetails auf dem Apple MDM-Standort konfiguriert werden müssen.

Alle MDMs

Diese Schritte gelten für die Bereitstellung in allen MDMs und müssen zuerst durchgeführt werden:

1. Stellen Sie sicher, dass Ihre Admin-E-Mail-Adresse im Dashboard unter der Option "Einstellungen" auf der Seite "Mobilgeräte" hinzugefügt wird.
2. Laden Sie die Datei `Cisco_Umbrella_Root_CA.cer` zur Verwendung auf dem iOS-Gerät herunter. Dieses Zertifikat ermöglicht errorlose HTTPS-Blockseiten. So rufen Sie die Stammzertifizierungsstelle ab:
    1. Navigieren Sie zu Deployments > Configuration > Root Certificate.
    2. Wählen Sie Zertifikat herunterladen aus.
    3. Speichern Sie den Download als `.cer` Datei.

MobileIron Cloud

Derzeit unterstützt der MobileIron-Download auf dem Dashboard nur die lokale Version. Die Cloud-Version verwendet andere Gerätevariablen als die Software vor Ort. Die Bereitstellung ähnelt stark der Bereitstellung am Standort, mit einigen Ausnahmen. MobileIron Core kann je nach Version diese Änderung erfordern.

So stellen Sie in MobileIron Cloud bereit:

1. Stellen Sie sicher, dass Ihre Admin-E-Mail-Adresse im Dashboard unter der Option "Einstellungen" auf der Seite "Mobilgeräte" hinzugefügt wird.
2. Laden Sie das Mobile Iron-Profil vom Umbrella Dashboard herunter.
3. Ersetzen Sie diese Variablen:

Generische Platzhaltervariable	Neue Variable
`"$DEVICE_SN$"`	`${deviceSN}`
`"$DEVICE_MAC$"`*	`${deviceWifiMacAddress}`

*Diese Einstellung wird nur für die Clarity-Komponente des CSC verwendet, nicht für die Umbrella-Komponente. Wenn Sie Clarity nicht verwenden, kann $DEVICE_MAC$ nicht ersetzt werden.

Citrix Endpoint Management-MDM

Führen Sie zur Bereitstellung auf Citrix die folgenden Vorbereitungsschritte im Dashboard aus:

1. Stellen Sie sicher, dass Ihre Admin-E-Mail-Adresse im Dashboard unter der Option "Einstellungen" auf der Seite "Mobilgeräte" hinzugefügt wird.

2. Laden Sie die generische MDM-Konfiguration von Umbrella herunter (AMP wird auf die gleiche Weise konfiguriert).
3. Laden Sie das Root-Zertifikat für Umbrella herunter:
    1. Navigieren Sie zu Deployments > Configuration > Root Certificate.
    2. Wählen Sie Zertifikat herunterladen aus.
    3. Speichern Sie den Download als `.cer` Datei.
4. Ändern Sie die Konfiguration, und ersetzen Sie den generischen Platzhalter durch die richtige Variable für den Citrix MDM:

Generische Platzhaltervariable	Neue Variable
`Seriennummer`	`${device.serialnumber}`
`MAC-Adresse*`	`${device.MAC_ADDRESS}`

*Diese Einstellung wird nur für die Clarity-Komponente des CSC verwendet, nicht für die Umbrella-Komponente.

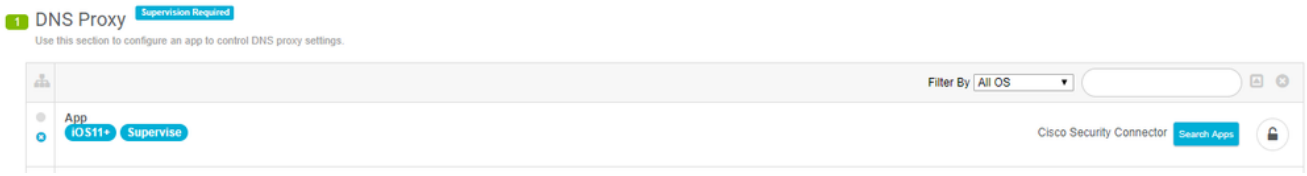
Führen Sie anschließend die folgenden MDM-Schritte aus:

1. Konfigurieren Sie den MDM so, dass er die CSC-Anwendung mithilfe von Apple Business Manager (ABM) installiert (früher bekannt als VPP, Volume Purchase Program).
2. Laden Sie die Umbrella- und/oder Clarity-Konfiguration hoch, die in den Vorbereitungsschritten geändert wurde.
3. Führen Sie die Schritte in der Citrix-Dokumentation aus, um das Profil zu importieren.
4. Laden Sie das Zertifikat für das Gerät hoch, um der Umbrella Root Certificate Authority zu vertrauen.
5. Konfigurieren Sie die Richtlinien, um Profile, eine CA und die 1 CSC-App an die erforderlichen Geräte zu senden.

Lightspeed-MDM

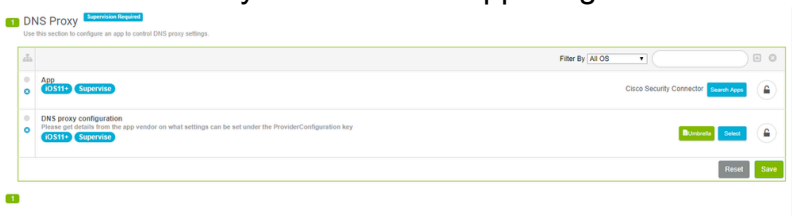
Lightspeed MDM unterstützt die textbasierte Konfiguration des iOS DNS-Proxys. Dies kann durch eine Änderung des generischen MDM-Profils erreicht werden.

1. Laden Sie die "generische Datei mobileconfig" herunter und ändern Sie die Dateierweiterung von .xml in .txt.
2. Öffnen Sie die Datei, und ändern Sie die Seriennummer des Platzhalters in Zeile 58 in `%serial_number%`.
3. Fügen Sie in Lightspeed dem DNS-Proxy-Profil die Cisco Security Connection wie abgebildet hinzu.



360019477192

4. Fügen Sie der Konfigurationsoption für den DNS-Proxy unterhalb der App die geänderte generische Mobileconfig-Datei hinzu.



360019477152

5. Laden Sie abschließend die Cisco Root CA von Umbrella herunter, und stellen Sie sie in Lightspeed bereit, um zertifizierungsfreie Blockseiten zu gewährleisten.

360019477132

Diese Schritte gelten für die Bereitstellung in allen MDMs. Führen Sie bitte zuerst diese Schritte aus.

JAMF Schulen

Die Bereitstellung von CSC mit JAMF Schools unterscheidet sich von JAMF. Beginnen Sie mit dem generischen Profil, und lesen Sie die Schritte in der JAMF-Dokumentation.

Im Folgenden finden Sie ein Beispiel für die Auswahl und die zu verwendende Variable für die Seriennummer:

```
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. Erstellen Sie ein neues Profil in der JAMF School.
   Weitere Informationen finden Sie in der JAMF-Dokumentation zu Geräteprofilen.
2. Verwenden Sie die DNS-Proxy-Nutzlast, um diese Einstellungen zu konfigurieren:
   1. Geben Sie im Feld App Bundle ID (Anwendungspaket-ID) `com.cisco.ciscosecurity.app` ein.
   2. Geben Sie im Feld Provider Bundle ID (Anbieterpaket-ID) `com.cisco.ciscosecurity.app.CiscoUmbrella` ein.
3. Fügen Sie die in Schritt 2 der JAMF-Dokumentation erstellte XML-Datei der Anbieterkonfiguration hinzu.

JAMF vor 10.2.0

Für die Bereitstellung des CSC mit JAMF sind umfangreiche Profiländerungen erforderlich. Führen Sie die folgenden Schritte aus, um das CSC mit JAMF MDM bereitzustellen.

1. Vergewissern Sie sich, dass Ihre Admin-E-Mail-Adresse dem Dashboard unter der Option Einstellungen auf der Seite für Mobilgeräte hinzugefügt wurde.
2. Umbrella-Stammzertifizierungsstelle hinzufügen:
   1. Navigieren Sie zu Deployments > Configuration > Root Certificate.
   2. Wählen Sie Zertifikat herunterladen aus.
   3. Speichern Sie den Download als CER-Datei.
   4. Geben Sie einen Namen für das Zertifikat an, und wählen Sie Zertifikat hochladen aus.
   5. Laden Sie die CER-Datei hoch, und lassen Sie das Kennwortfeld leer.
   6. Wenden Sie sich an den Bereich Ihrer Geräte, um dieses Zertifikat zu verteilen.
3. Laden Sie das generische Profil vom Umbrella Dashboard herunter.
4. Wenn Sie JAMF Pro v.10.2.0 oder höher verwenden, können Sie diesen Schritt überspringen. Sie können das fertige Format importieren, indem Sie Folgendes hinzufügen:

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

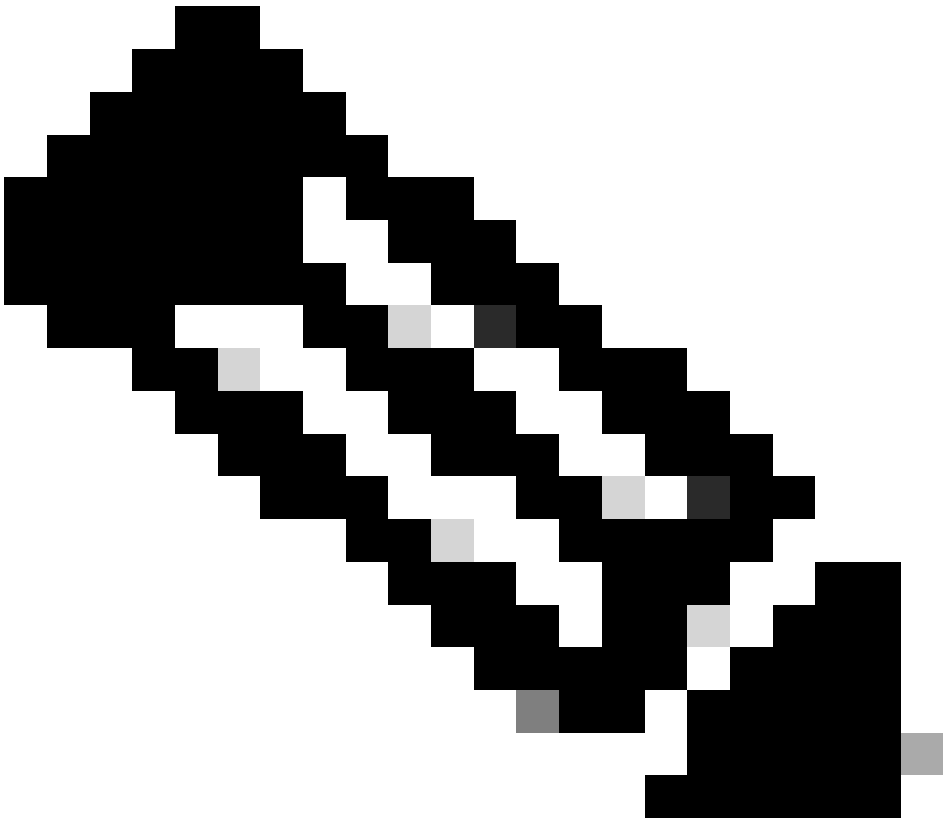
5. Wenn Sie eine JAMF-Version vor v.10.2.0 verwenden, bearbeiten Sie das XML-Profil ausführlich, wie in diesem Beispielprofil gezeigt. Kopieren Sie dieses Beispiel nicht, es

funktioniert nicht wie es ist. Verwenden Sie nur die generische Download-Konfiguration auf Ihrem Dashboard.

```
<?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. In JAMF importieren:
    1. Klicken Sie im Hauptfenster der MDM-Konfiguration auf Neu, um ein neues Profil zu erstellen.



Anmerkung: Dabei muss es sich um ein separates Profil handeln, das nicht zusammen mit dem erstellten Zertifikatprofil verwendet werden darf. Damit die App funktioniert, müssen diese beiden Profile separat auf das Gerät geschoben werden.

2. Geben Sie dem Profil einen Namen, und navigieren Sie zu DNS-Proxy.
3. Klicken Sie unter dem DNS-Proxy auf Konfigurieren.
4. Setzen Sie die Proxy-Konfiguration auf Umbrella details:

    1. Geben Sie im Feld App Bundle ID (Anwendungspaket-ID) `com.cisco.ciscosecurity.app ein`.

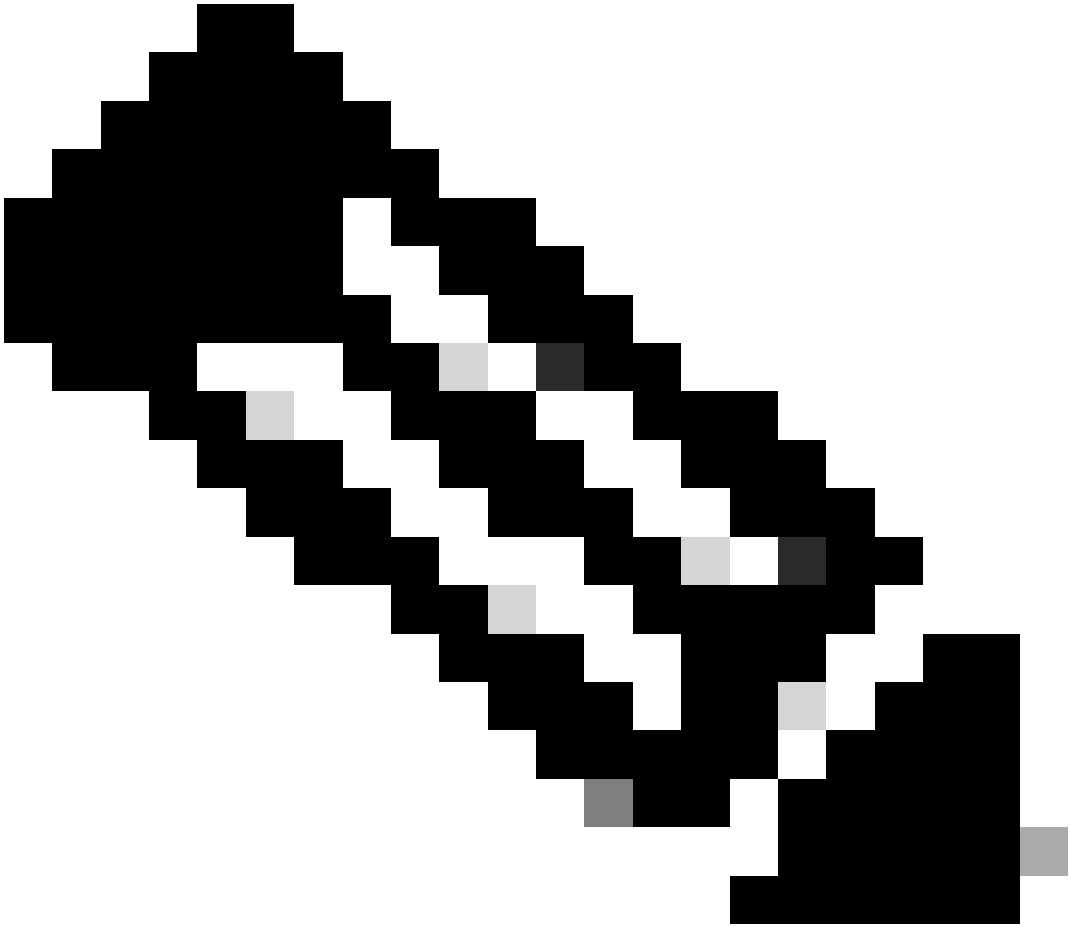
    2. Geben Sie in das Feld Provider Bundle ID (Anbieterpaket-ID) Folgendes ein: `com.cisco.ciscosecurity.app.CiscoUmbrella`.

    3. Fügen Sie den bearbeiteten XML-Inhalt aus Umbrella ein.
    in die Anbieterkonfiguration
    XML-Abschnitt.

5. Klicken Sie auf Bereich, und wenden Sie den richtigen Bereich von Geräten an.

InTune

InTune wird direkt zum Umbrella Dashboard hinzugefügt. Weitere Informationen finden Sie in der Umbrella InTune-Dokumentation.



> Anmerkung: Clarity ist ein Produkt von Cisco AMP für Endgeräte. Wenn Sie derzeit nicht für dieses Produkt lizenziert sind, überspringen Sie den entsprechenden Abschnitt zur Einrichtung.

Mosyle

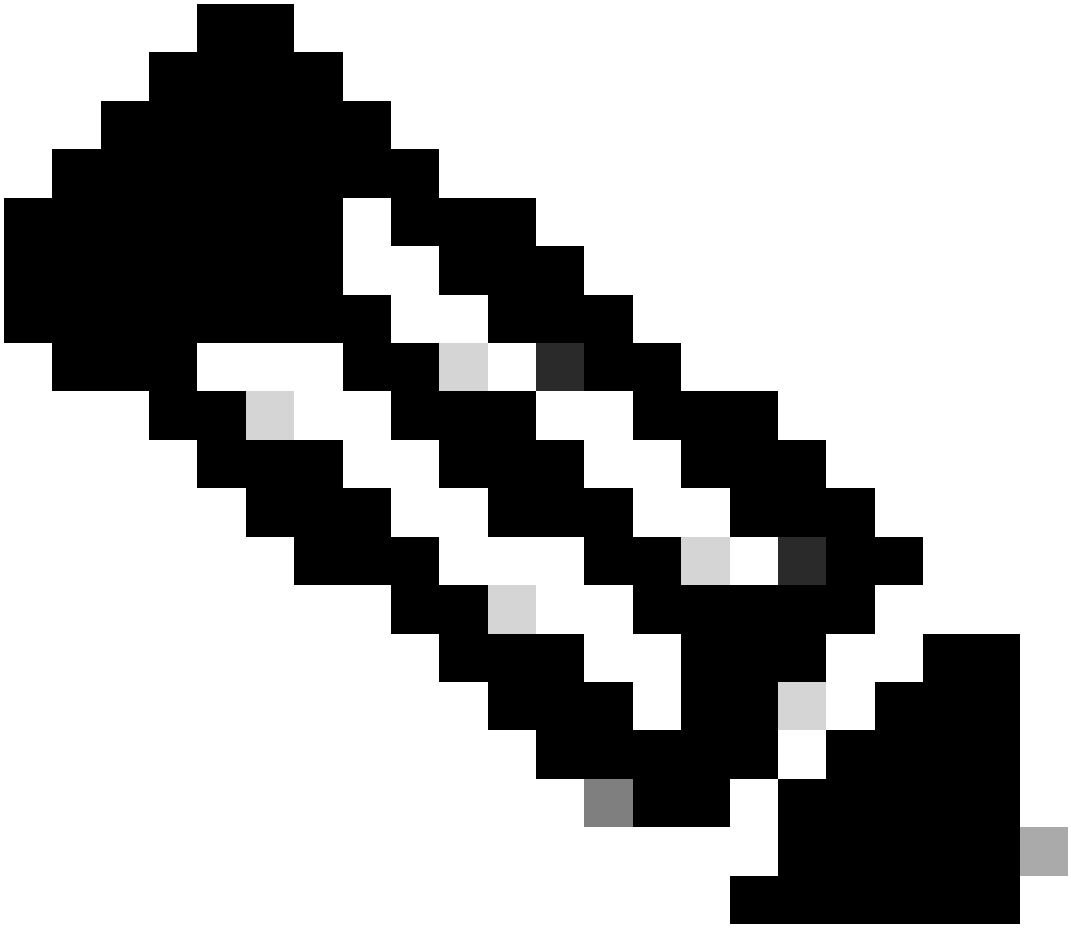
Die Unterstützung für Module erfolgt über die Konfiguration des DNS-Proxys:

- Geben Sie im Feld App Bundle ID (Anwendungspaket-ID) `com.cisco.ciscosecurity.app ein`.
- Geben Sie in das Feld Provider Bundle ID (Anbieterpaket-ID) Folgendes ein: `com.cisco.ciscosecurity.app.CiscoUmbrella`

.

Fügen Sie den Inhalt im XML`<key>ProviderConfiguration</key>`-Feld zum Feld Mossle Provider Configuration hinzu:

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



Anmerkung: Für die Einstellungen müssen die Geräte konfiguriert werden, damit sie die Konfiguration empfangen können, und die Bereiche werden nicht standardmäßig hinzugefügt.

Sicher

Konfigurieren Sie die Sicherheit auf der DNS-Proxy-Profilseite:

- Geben Sie im Feld "App Bundle ID" `com.cisco.ciscosecurity.app ein.`
- Geben Sie im Feld Provider Bundle ID (Anbieterpaket-ID) `com.cisco.ciscosecurity.app.CiscoUmbrella` ein.

Führen Sie die folgenden Schritte aus, um die Datei `.plist` zu konfigurieren:

1. Beginnen Sie mit der iOS Common Config-Vorlage, und bearbeiten Sie die Datei in einer `.plist`, wobei nur die `<dict>` bis `</dict>` in den `<key>ProviderConfiguration</key>` Kommentaren angezeigt wird.
2. Ersetzen Sie den `serialNumber`-Schlüssel durch die `Seriennummer`-Variable `$`, wie von Security definiert.
3. Der Inhalt der Datei `.plist` kann diesem Beispiel sehr ähnlich sein. Laden Sie diesen in die DNS-Proxy-Konfiguration hoch:

```
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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.