

追加のMDMプラットフォームでのiOS用CSCの展開

内容

[はじめに](#)

[背景説明](#)

[すべてのMDM](#)

[MobileIronクラウド](#)

[Citrix Endpoint Management MDM](#)

[光速度MDM](#)

[JAMFスクール](#)

[JAMF 10.2.0より前](#)

[インチューン](#)

[モデル](#)

[安全に](#)

はじめに

このドキュメントでは、追加のモバイルデバイス管理プラットフォームでiOS用Cisco Security Connector(CSM)を導入する方法について説明します。

背景説明

[Cisco Security Connector\(CSC\)for iOS](#)は、iPhoneに対する包括的なDNS保護です。このガイドを展開に使用する前に、[CSC展開ドキュメント](#)を参照してください。CSCを使用するには、デバイスが監視モードである必要があります。

このドキュメントでは、CSCに対するその他のMobile Device Management(MDM)ソフトウェアサポートの概要を説明します。これらのMDMは、正常に導入されたことによって検証されていますが、まだダッシュボードに直接表示されていません。

iOSデバイスにプロファイルが存在することを確認するには、次の手順を実行します。

1. Settings > General > Device Management > [MDM Profile Name] > More detailsの順に選択します。
2. プロファイルタイプDNSプロキシが次の詳細情報とともに存在することを確認します。
 - アプリの詳細：com.cisco.ciscosecurity.app
 - プロバイダーバンドルの詳細：com.cisco.ciscosecurity.ciscoumbrella

[Apple MDMサイトで設定するiOSプロファイルの詳細を確認してください。](#)

すべてのMDM

次の手順は、すべてのMDMへの導入に適用され、最初に完了する必要があります。

1. 管理用電子メールアドレスがダッシュボードの[モバイルデバイス]ページの[設定]オプションに追加されていることを確認します。
2. iOSデバイスで使用するCisco_Umbrella_Root_CA.cerファイルをダウンロードします。この証明書により、エラーのないHTTPSブロックページが可能になります。ルートCAを取得するには、次の手順を実行します。
 1. Deployments > Configuration > Root Certificateの順に選択します。
 2. Download Certificateを選択します。
 3. ダウンロードを.cerファイルとして保存します。

MobileIronクラウド

現在、ダッシュボードでのMobileIronのダウンロードは、オンプレミスバージョンのみをサポートしています。クラウドバージョンは、オンプレミスソフトウェアとは異なるデバイス変数を使用します。導入は、いくつかの例外を除いて、オンプレミスと非常によく似ています。バージョンに応じてMobileIron Coreを変更する必要があります。

MobileIron Cloudに導入するには、次の手順を実行します。

1. 管理用電子メールアドレスがダッシュボードの[モバイルデバイス]ページの[設定]オプションに追加されていることを確認します。
2. UmbrellaダッシュボードからMobile Ironプロファイルをダウンロードします。
3. 次の変数を置き換えます。

汎用プレースホルダ変数	新しい変数
"\$DEVICE_SN\$"	\${deviceSN}
"\$DEVICE_MAC\$"*	\${deviceWifiMacAddress}

* これはCSCのClarityコンポーネントでのみ使用され、Umbrellaコンポーネントでは使用されません。Clarityを使用しない場合、置き換える\$DEVICE_MAC\$はありません。

Citrix Endpoint Management MDM

Citrixに展開するには、ダッシュボードで次の準備手順を実行します。

1. 管理用電子メールアドレスがダッシュボードの[モバイルデバイス]ページの[設定]オプションに追加されていることを確認します。
2. [Umbrellaから汎用MDM設定](#)をダウンロードします (AMPも同様に設定します)。
3. Umbrellaのルート証明書をダウンロードします。

1. Deployments > Configuration > Root Certificateの順に選択します。
2. Download Certificateを選択します。
3. ダウンロードを.cerファイルとして保存します。
4. 設定を変更し、汎用プレースホルダを[Citrix MDM](#)用の正しい変数に置き換えます。

汎用プレースホルダ変数	新しい変数
serial_number	\${device.serialnumber}
MACアドレス*	\${device.MAC_ADDRESS}

* これはCSCのClarityコンポーネントでのみ使用され、Umbrellaコンポーネントでは使用されません。

次に、次のMDM手順を実行します。

1. Apple Business Manager(ABM) (旧称VPP、Volume Purchase Program) を使用してCSCアプリをインストールするようにMDMを設定します。
2. 準備手順で変更したUmbrellaまたはClarityの設定をアップロードします。
3. [Citrixのドキュメントの手順を使用してプロファイルをインポートします。](#)
4. [Umbrellaルート認証局](#)を信頼するデバイスの証明書をアップロードします。
5. プロファイル、1つのCA、および1つのCSCアプリケーションを必要なデバイスにプッシュするようにポリシーを設定します。

光速度MDM

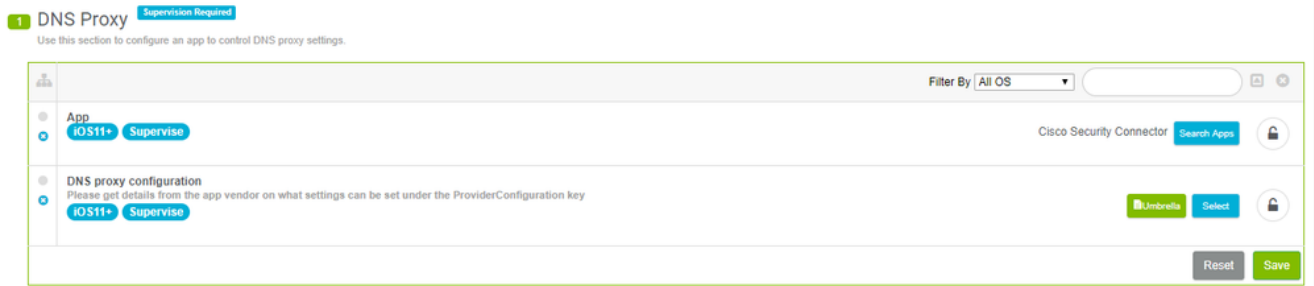
Lightspeed MDMは、iOS DNSプロキシのテキストベースの設定をサポートします。これは、汎用MDMプロファイルを変更することで実現できます。

1. 「generic mobileconfig file」をダウンロードし、ファイル拡張子を.xmlから.txtに変更します。
2. ファイルを開き、58行目のプレースホルダシリアル番号の文字列を%serial_number%
3. Lightspeedで、次に示すようにDNSプロキシプロファイルにCisco Security Connectionを追加します



360019477192

4. 変更した汎用mobileconfigファイルを、アプリケーションの下にDNSプロキシ設定オプションに追加します。



1

360019477152

5. 最後に、Umbrellaから[CiscoルートCA](#)をダウンロードし、Lightspeedに展開して、証明書な

しのブロックページを確保します。



360019477132

次の手順は、すべてのMDMへの導入に適用されます。最初にこれらの手順を使用してください。

JAMFスクール

JAMF Schoolsを使用したCSCの導入は、JAMFとは異なります。一般的なプロファイルから始めて、[JAMFドキュメント](#)の手順を参照してください。

選択する場所とシリアル番号に使用する変数の設定例を次に示します。

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. JAMF Schoolで新しいプロファイルを作成します。
詳細については、[デバイスプロファイルに関するJAMFのドキュメント](#)を参照してください。
2. DNSプロキシペイロードを使用して、次の設定を行います。
 1. App Bundle IDフィールドに、com.cisco.ciscosecurity.appと入力します。
 2. Provider Bundle IDフィールドに、com.cisco.ciscosecurity.app.CiscoUmbrellaと入力します。
3. 「[JAMFに関する文書](#)」のステップ2で作成したXMLファイルをプロバイダー設定に追加します。

JAMF 10.2.0より前

JAMFを使用してCSCを導入するには、プロファイルを大幅に変更する必要があります。JAMF MDMを使用してCSCを導入するには、次の手順を使用します。

1. 管理用電子メールアドレスが、モバイルデバイスページの設定オプションの下ダッシュボードに追加されていることを確認します。
2. UmbrellaルートCAを追加します。
 1. Deployments > Configuration > Root Certificateの順に選択します。
 2. Download Certificateを選択します。
 3. ダウンロードを.cerファイルとして保存します。
 4. 証明書の名前を入力し、Upload Certificateを選択します。
 5. .cerをアップロードし、パスワードフィールドは空白のままにします。
 6. この証明書をプッシュするデバイスの範囲に適用します。
3. Umbrellaダッシュボードから汎用プロファイルをダウンロードします。
4. JAMF Pro v.10.2.0以降を使用している場合は、この手順を省略できます。次を追加して、そのままインポートできます。

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

5. v.10.2.0より前のJAMFバージョンを使用している場合は、このプロファイル例に示すようにXMLプロファイルを大幅に編集します。この例はコピーしないでください。現在の状態で

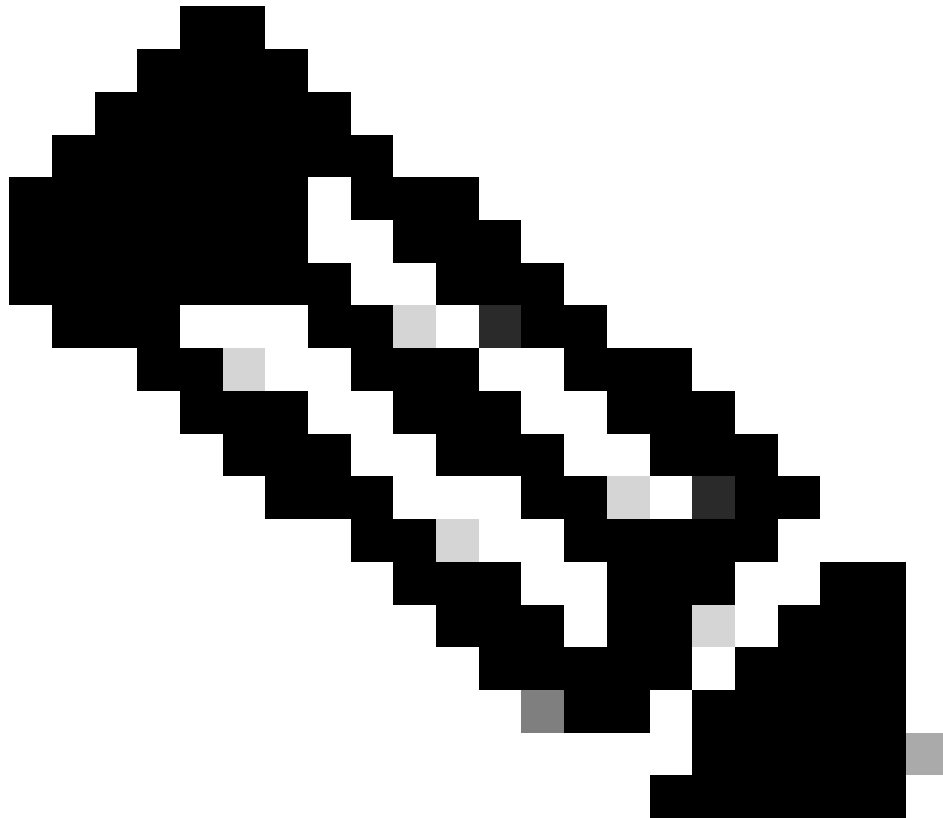
は機能しません。ダッシュボードからの一般的なダウンロード設定のみを使用します。

```
<?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.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. JAMFにインポート：

1. MDMのメイン設定ウィンドウで、Newをクリックして新しいプロファイルを作成します。

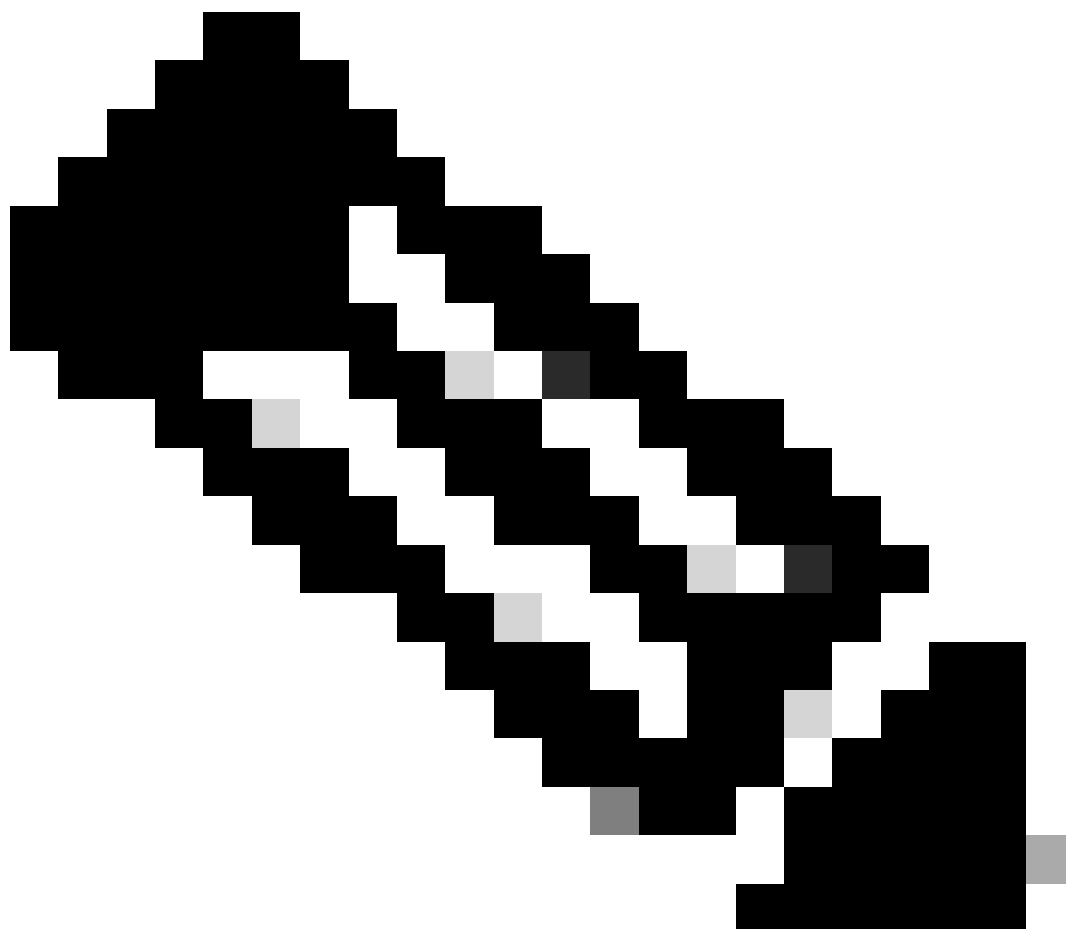


注：これは別のプロファイルにする必要があり、作成した証明書プロファイルと併用しないでください。アプリが機能するためには、これら2つのプロファイルを個別にデバイスにプッシュする必要があります。

-
2. プロファイルに名前を付け、DNS Proxyに移動します。
 3. DNSプロキシでConfigureをクリックします。
 4. プロキシ設定をUmbrellaの詳細に設定します。
 1. App Bundle IDフィールドに、`com.cisco.ciscosecurity.app`と入力します。
 2. Provider Bundle IDフィールドに、`com.cisco.ciscosecurity.app.CiscoUmbrella`を選択します。
 3. 編集したXMLコンテンツをUmbrellaから貼り付けるプロバイダー設定に追加します。
XMLセクション。
 5. Scopeをクリックして、デバイスの適切な範囲に適用します。

インチューン

InTuneはUmbrellaダッシュボードに直接追加されます。詳細については、[Umbrella InTuneに関するドキュメント](#)を参照してください。



注:ClarityはCisco AMP for Endpointsの製品です。この製品のライセンスを取得していない場合は、関連するセットアップ部分を省略してください。

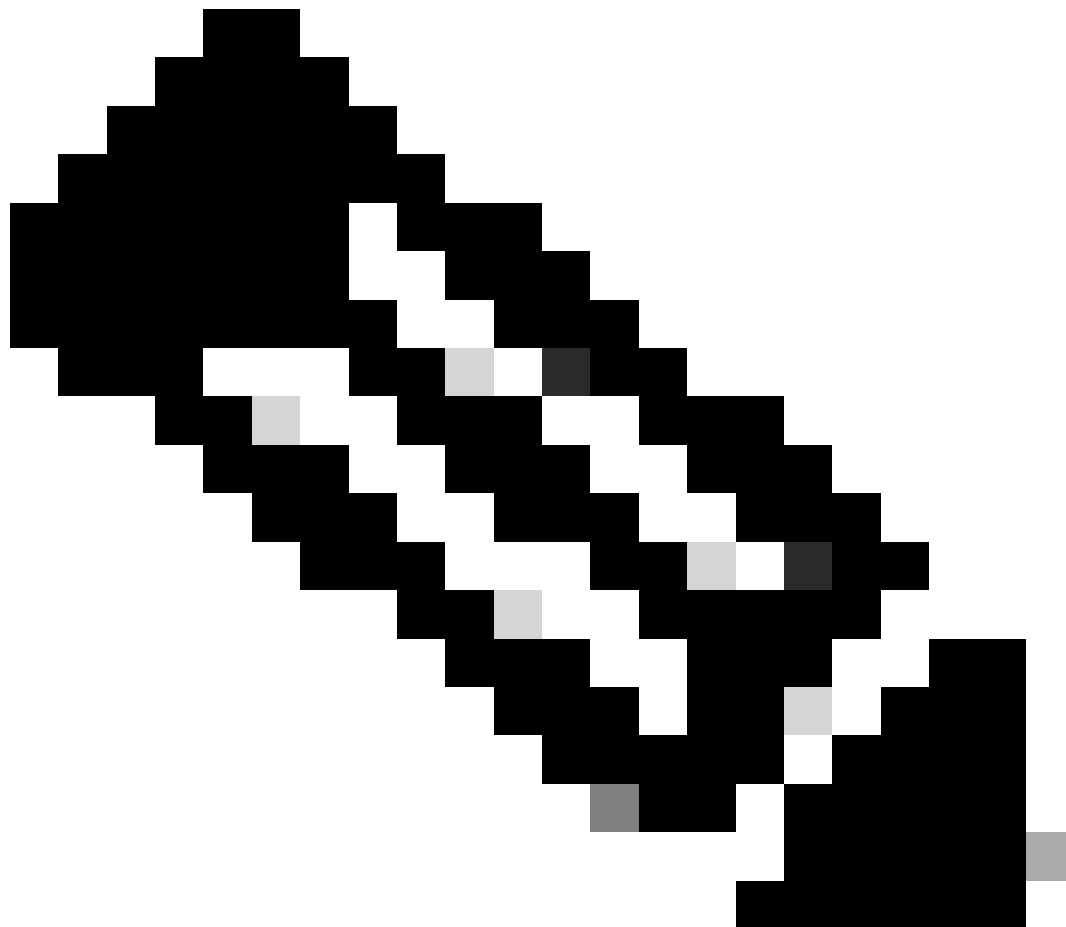
モデル

Mosyleのサポートは、DNSプロキシ設定の形式で行われます。

- App Bundle IDフィールドに、`com.cisco.ciscosecurity.app`と入力します。
- Provider Bundle IDフィールドに、`com.cisco.ciscosecurity.app.CiscoUmbrella`を選択します。

XML `<key>ProviderConfiguration</key>`内のコンテンツをMosyle Provider Configurationフィールドに追加します。

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



注：この設定では、設定を受信するためにデバイスのスコープを設定する必要があります。デフォルトでは、スコープは追加されません。

安全に

DNS Proxy profileページでSecurityを設定します。

- App Bundle IDフィールドに、com.cisco.ciscosecurity.appと入力します。

- Provider Bundle IDフィールドに、com.cisco.ciscosecurity.app.CiscoUmbrellaと入力します。

.plistファイルを設定するには、次の手順を使用します。

1. 最初にiOS Common Configテンプレートを使用し、<dict> ~ </dict>のみを含む.plistファイルを<key>ProviderConfiguration</key>コメント内で編集します。
2. serialNumberキーを、Securlyで定義されている\$serialnumber変数[に置き換えます](#)。
3. .plistファイルの内容は、この例とよく似ている可能性があります。これをDNSプロキシ設定にアップロードします。

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

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。