

Implementeer CSC voor iOS op extra MDM-platforms

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[Alle MDM's](#)

[MobileIron Cloud](#)

[Citrix Endpoint Management MDM](#)

[Lightspeed MDM](#)

[JAMF Schools](#)

[JAMF eerder dan 10.2.0](#)

[op maat maken](#)

[Mosyle](#)

[stevig](#)

Inleiding

In dit document wordt beschreven hoe u Cisco Security Connector voor iOS kunt implementeren op aanvullende beheerplatforms voor mobiele apparaten.

Achtergrondinformatie

De [Cisco Security Connector \(CSC\) voor iOS](#) is volledig Umbrella DNS-bescherming voor uw iPhone. Lees de [documentatie](#) van de [CSC-implementatie voordat u](#) deze handleiding voor implementaties gebruikt. Uw apparaat moet zich in de gecontroleerde modus bevinden om de CSC te kunnen gebruiken.

In dit document wordt een overzicht gegeven van de aanvullende MDM-softwareondersteuning (Mobile Device Management) voor de CSC. Deze MDM's zijn gevalideerd door een succesvolle implementatie, maar zijn nog niet direct aanwezig op het Dashboard.

Controleren of er een profiel op een iOS-apparaat bestaat:

1. Ga naar Instellingen > Algemeen > Apparaatbeheer > [MDM-profielnaam] > Meer details.
2. Bevestig dat het profieltype DNS Proxy aanwezig is, samen met de volgende details:
 - App-details: com.cisco.ciscosecurity.app
 - Aanbieder bundelgegevens: com.cisco.ciscosecurity.ciscoumbrella

[Lees meer over welke iOS-profielgegevens u moet configureren op de Apple MDM-site.](#)

Alle MDM's

Deze stappen gelden voor implementatie op alle MDM's en moeten eerst worden voltooid:

1. Zorg ervoor dat het e-mailadres van uw beheerder wordt toegevoegd aan het dashboard onder de optie "Instellingen" op de pagina Mobiele apparaten.
2. Download het `Cisco_Umbrella_Root_CA.cer` bestand voor gebruik op het iOS apparaat. Dit certificaat maakt foutloze HTTPS-blokpagina's mogelijk. Om de Root CA te verkrijgen:
 1. Navigeer naar Implementaties > Configuratie > Hoofdcertificaat.
 2. Selecteer Certificaat downloaden.
 3. Sla de download op als een `.cer` bestand.

MobileIron Cloud

Momenteel ondersteunt de MobileIron-download op het dashboard alleen de on-premise versie. De cloudversie gebruikt andere apparaatvariabelen dan de on-premise software. De implementatie is vergelijkbaar met on-premise, met verschillende uitzonderingen. MobileIron Core kan afhankelijk van de versie deze wijziging vereisen.

Implementeren naar MobileIron Cloud:

1. Zorg ervoor dat het e-mailadres van uw beheerder wordt toegevoegd aan het dashboard onder de optie "Instellingen" op de pagina Mobiele apparaten.
2. Download het Mobile Iron profiel van het Umbrella dashboard.
3. Vervang deze variabelen:

Generieke plaatsaanduidingsvariabele	Nieuwe variabele
"\$DEVICE_SN\$"	<code>\${deviceSN}</code>
"\$DEVICE_MAC\$"*	<code>\${deviceWiFiMacAddress}</code>

*Dit wordt alleen gebruikt voor de Clarity component van de CSC, niet voor de Umbrella component. Als u Clarity niet gebruikt, is er geen `$DEVICE_MAC$` te vervangen.

Citrix Endpoint Management MDM

Voer de volgende voorbereidingsstappen uit in het dashboard om te implementeren in Citrix:

1. Zorg ervoor dat het e-mailadres van uw beheerder wordt toegevoegd aan het dashboard onder de optie "Instellingen" op de pagina Mobiele apparaten.
2. Download de [generieke MDM-configuratie van Umbrella](#) (AMP is op dezelfde manier geconfigureerd).
3. Download het root certificaat voor Umbrella:

1. Ga naar Implementaties > Configuratie > Hoofdcertificaat.
2. Selecteer Certificaat downloaden.
3. Sla de download op als een .cer bestand.
4. Wijzig de configuratie en vervang de algemene plaatsaanduiding door de juiste variabele voor de [Citrix MDM](#):

Generieke plaatsaanduidingsvariabele	Nieuwe variabele
Serial_Number	\${apparaat.serienummer}
MAC_Adres*	\${device.MAC_ADDRESS}

*Dit wordt alleen gebruikt voor de Clarity component van de CSC, niet voor de Umbrella component.

Voer vervolgens deze MDM-stappen uit:

1. Configureer de MDM om de CSC-app te installeren met Apple Business Manager (ABM) (voorheen bekend als VPP, Volume Purchase Program).
2. Upload de gewijzigde Umbrella- en/of Clarity-configuratie in de voorbereidingsstappen.
3. [Gebruik de stappen in de Citrix-documentatie om het profiel te importeren.](#)
4. Upload het certificaat voor het apparaat om de [Umbrella Root Certificate Authority](#) te vertrouwen.
5. Configureer het beleid om de profielen, 1 CA en de 1 CSC-app naar het (de) gewenste apparaat(en) te pushen.

Lightspeed MDM

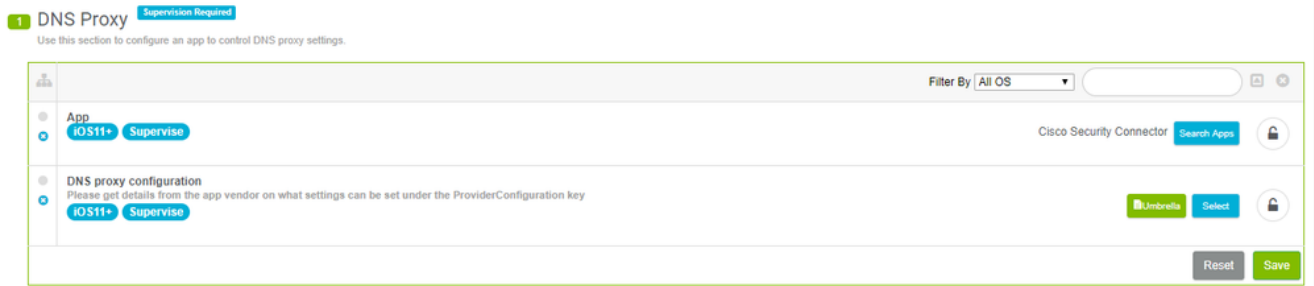
Lightspeed MDM ondersteunt tekstgebaseerde configuratie van de iOS DNS-proxy. Dit kan worden bereikt door het algemene MDM-profiel aan te passen.

1. Download het "generic mobileconfig file" en wijzig de bestandsextensie van .xml naar .txt.
2. Open het bestand en wijzig de tekenreeks met het serienummer voor de plaatsaanduiding op regel 58 in %serial_number%
3. Voeg in Lightspeed de Cisco-beveiligingsverbinding toe aan het DNS-proxyprofiel, zoals wordt weergegeven



360019477192

4. Voeg het gewijzigde generieke mobileconfig-bestand toe aan de optie DNS-proxyconfiguratie onder de app.

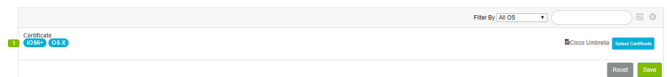


1

360019477152

5. Download ten slotte de [Cisco Root CA](#) van Umbrella en implementeer deze in Lightspeed

om certificaatvrije blokpagina's te garanderen.



360019477132

Deze stappen zijn van toepassing op implementatie op alle MDM's. Gebruik deze stappen eerst.

JAMF Schools

Het inzetten van CSC met JAMF Schools verschilt van JAMF. Begin met het algemene profiel en bekijk de stappen in de [JAMF-documentatie](#).

Hier is een voorbeeldconfiguratie van waar te selecteren en welke variabele te gebruiken voor het serienummer:

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. Maak een nieuw profiel aan in JAMF School.
Zie de [JAMF-documentatie bij Apparaatprofielen voor](#) meer informatie.
2. Gebruik de DNS Proxy-payload om deze instellingen te configureren:
 1. Voer in het veld App Bundle ID het veld `com.cisco.ciscosecurity.app` in.
 2. Voer in het veld Provider Bundle ID het veld `com.cisco.ciscosecurity.app.CiscoUmbrella` in.
3. Voeg het XML-bestand dat u hebt gemaakt in stap 2 van de [JAMF-documentatie](#) toe aan de providerconfiguratie.

JAMF eerder dan 10.2.0

Het implementeren van de CSC met JAMF vereist aanzienlijke profielwijzigingen. Gebruik deze stappen om de CSC met JAMF MDM te implementeren.

1. Zorg ervoor dat het e-mailadres van uw beheerder wordt toegevoegd aan het dashboard onder de optie Instellingen voor mobiele apparaten.
2. Voeg de Umbrella root CA toe:
 1. Ga naar Implementaties > Configuratie > Hoofdcertificaat.
 2. Selecteer Certificaat downloaden.
 3. Sla de download op als een .cer-bestand.
 4. Geef een naam op voor het certificaat en selecteer Certificaat uploaden.
 5. Upload de .cer en laat het wachtwoord veld leeg.
 6. Pas dit toe op het bereik van uw apparaten om dit certificaat te verwijderen.
3. Download het generieke profiel van het Umbrella dashboard.
4. Als u JAMF Pro v.10.2.0 of hoger gebruikt, kunt u deze stap overslaan. U kunt as-is importeren door deze toe te voegen:

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

5. Als u een JAMF-versie eerder dan v.10.2.0 gebruikt, bewerkt u het XML-profiel uitgebreid zoals in dit voorbeeldprofiel wordt weergegeven. Kopieer dit voorbeeld niet, het is niet functioneel zoals het is. Gebruik alleen de algemene downloadconfiguratie van uw

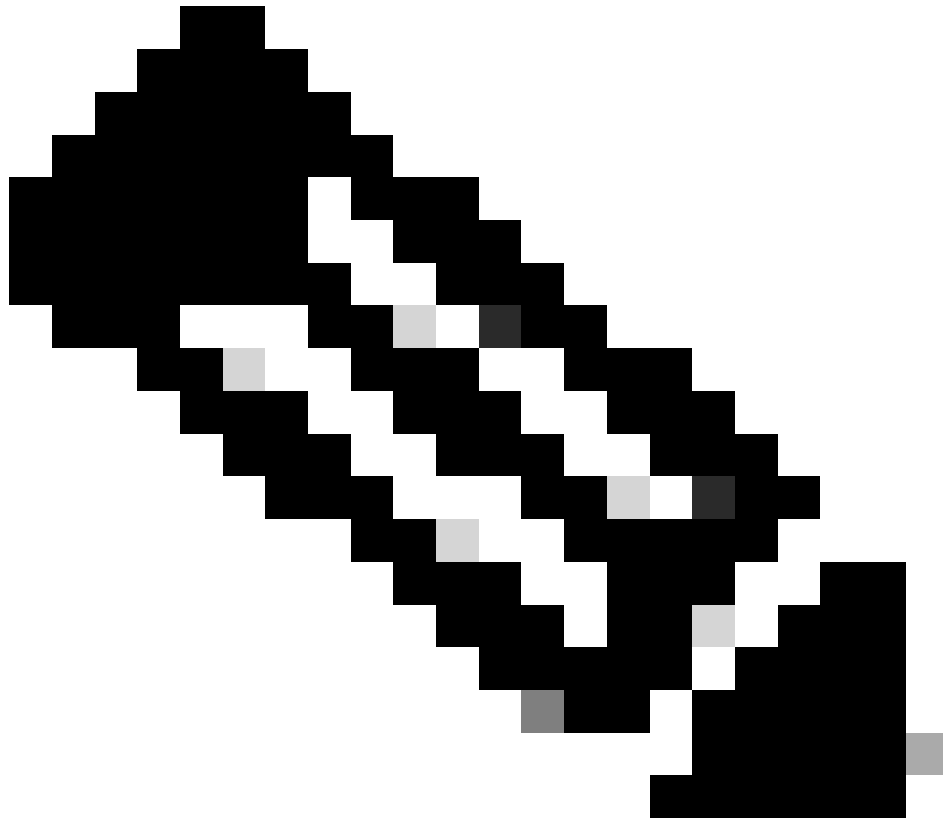
dashboard.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.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. Importeren naar JAMF:

1. Klik in het hoofdvenster van de MDM-configuratie op Nieuw om een nieuw profiel te maken.

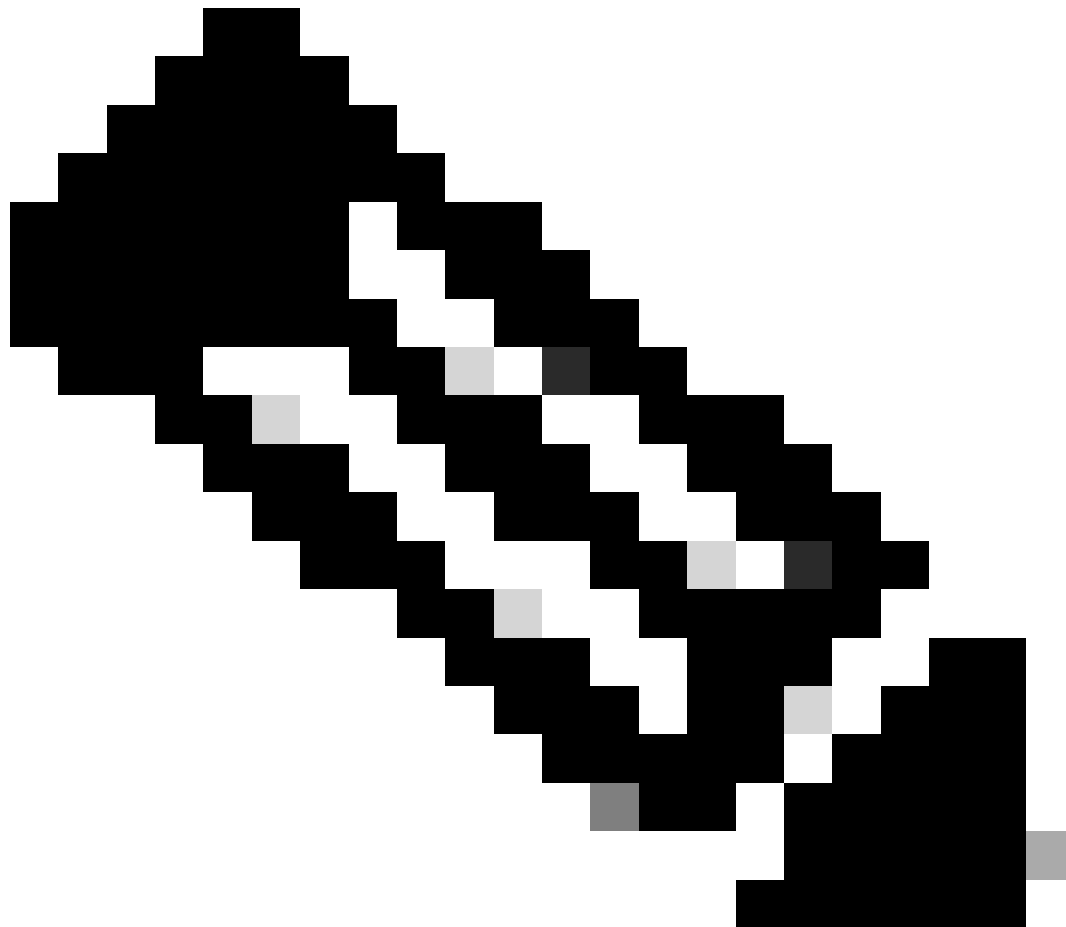


Opmerking: dit moet een apart profiel zijn en mag niet worden gebruikt met het aangemaakte certificaatprofiel. Om de app te laten werken, moeten deze twee profielen afzonderlijk naar het apparaat worden geduwd.

-
2. Geef het profiel een naam en navigeer naar DNS Proxy.
 3. Klik onder de DNS-proxy op Configureren.
 4. Stel de proxyconfiguratie in op Umbrella-details:
 1. Voer in het veld App Bundle ID het veld `com.cisco.ciscosecurity.app` in.
 2. Voer in het veld Provider Bundle ID het volgende in
`com.cisco.ciscosecurity.app.CiscoUmbrella`.
 3. De bewerkte XML-inhoud plakken vanuit Umbrella in de providerconfiguratie XML-sectie.
 5. Klik op Bereik en pas het juiste bereik van apparaten toe.

op maat maken

InTune wordt direct toegevoegd aan het Umbrella dashboard. Bekijk de [documentatie](#) van [Umbrella InTune](#) voor meer informatie.



Opmerking: Clarity is een product van Cisco AMP voor Eindpunten. Als u momenteel geen licentie hebt voor dit product, slaat u het bijbehorende installatiegedeelte over.

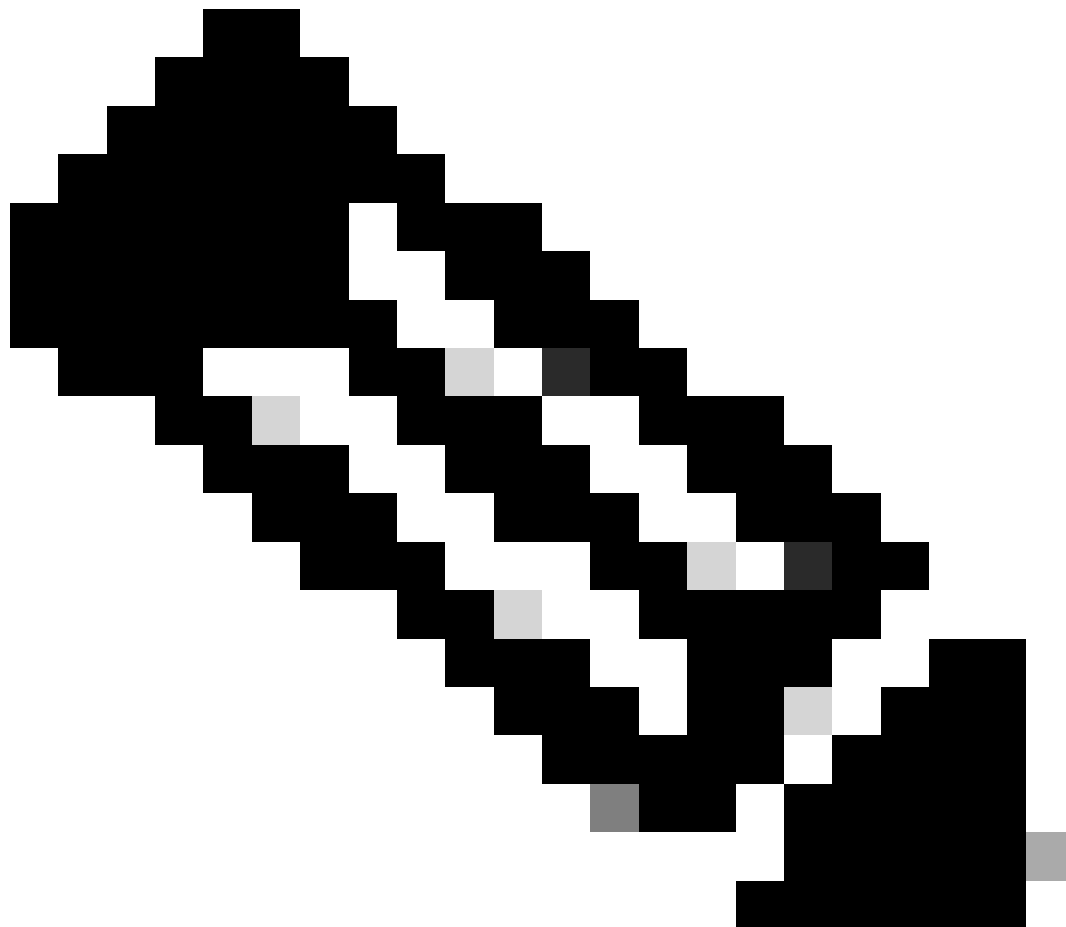
Mosyle

Mosyle ondersteuning is in de vorm van de DNS Proxy configuratie:

- Voer in het veld App Bundle ID het veld `com.cisco.ciscosecurity.app` in.
- Voer in het veld Provider Bundle ID het volgende in `com.cisco.ciscosecurity.app.CiscoUmbrella`.

Voeg de inhoud in het XML `<key>ProviderConfiguration</key>` toe aan het veld Mosyle Provider Configuration:

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



Opmerking: De instellingen vereisen dat de apparaten worden gescand om de configuratie te ontvangen en scopes worden niet standaard toegevoegd.

stevig

Veilig configureren op de profielpagina van DNS Proxy:

- Voer in het veld App Bundle ID het veld `com.cisco.ciscosecurity.app` in

- In het veld Provider Bundle ID voert u `com.cisco.ciscosecurity.app.CiscoUmbrella` in

Gebruik deze stappen om het bestand `.plist` te configureren:

1. Begin met de sjabloon voor algemene configuratie van iOS en bewerk het bestand in een `.plist` met alleen de `<dict>` via `</dict>` in de `<key>ProviderConfiguration</key>` opmerkingen.
2. Vervang de sleutel `SerialNumber` door de variabele `$serienummer`, [zoals gedefinieerd door Secure](#).
3. De `.plist` bestandsinhoud kan erg lijken op dit voorbeeld. Upload dit naar de DNS-proxyconfiguratie:

`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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.