Distribuzione di CSC per iOS su piattaforme MDM aggiuntive

Sommario

Introduzione

In questo documento viene descritto come distribuire Cisco Security Connector per iOS su piattaforme aggiuntive di gestione di dispositivi mobili.

Premesse

Cisco Security Connector (CSC) per iOS è una protezione DNS Umbrella completa per il tuo iPhone. Prima di utilizzare questa guida per le distribuzioni, consultare la documentazione relativa alla distribuzione di CSC. Per utilizzare CSC, il dispositivo deve essere in modalità di supervisione.

Questo documento riepiloga il supporto aggiuntivo del software di gestione dei dispositivi mobili (MDM) per CSC. Questi MDM sono stati convalidati da una distribuzione riuscita ma non sono ancora presenti direttamente nel dashboard.

Per verificare l'esistenza di un profilo su un dispositivo iOS:

1. Passare a Impostazioni > Generale > Gestione dispositivi > [Nome profilo MDM] > Ulteriori dettagli.
2. Confermare che il tipo di profilo Proxy DNS sia presente insieme ai seguenti dettagli:
    - Dettagli app: `com.cisco.ciscosecurity.app`
    - Dettagli bundle provider: `com.cisco.ciscosecurity.ciscoumbrella`

Ulteriori informazioni sui dettagli del profilo iOS da configurare nel sito MDM di Apple.

Tutti i MDM

I passi riportati di seguito si applicano alla distribuzione in tutti gli MDM e devono essere completati per primi.

1. Assicurarsi che l'indirizzo e-mail dell'amministratore sia aggiunto al dashboard nella pagina Dispositivi mobili "Impostazioni".
2. Scaricare il file `Cisco_Umbrella_Root_CA.cer` per utilizzarlo sul dispositivo iOS. Questo certificato consente pagine di blocco HTTPS senza errori. Per ottenere la CA radice:
    1. Passare a Distribuzioni > Configurazione > Certificato radice.
    2. Selezionare Scarica certificato.
    3. Salvare il download come file `.cer`.

MobileIron Cloud

Al momento, il download di MobileIron sul dashboard supporta solo la versione locale. La versione Cloud usa variabili di dispositivo diverse dal software in sede. La distribuzione è molto simile a quella in loco, con diverse eccezioni. MobileIron Core a seconda della versione può richiedere questa modifica.

Per eseguire la distribuzione in MobileIron Cloud:

1. Assicurarsi che l'indirizzo e-mail dell'amministratore sia aggiunto al dashboard nella pagina Dispositivi mobili "Impostazioni".
2. Scarica il profilo di Mobile Iron dal dashboard Umbrella.
3. Sostituire le seguenti variabili:

Variabile segnaposto generica	Nuova variabile
`"$DEVICE_SN$"`	`${snPeriferica}`
`"$DEVICE_MAC$"`*	`${indirizzoMacWifidispositivo}`

*Si usa solo per il componente Clarity del CSC, non per il componente Umbrella. Se non si utilizza Clarity, non vi sono $DEVICE_MAC$ da sostituire.

MDM Citrix Endpoint Management

Per la distribuzione su Citrix, completare i seguenti passaggi di preparazione nel dashboard:

1. Assicurarsi che l'indirizzo e-mail dell'amministratore sia aggiunto al dashboard nella pagina Dispositivi mobili "Impostazioni".
2. Scaricare la configurazione MDM generica da Umbrella (AMP è configurato allo stesso modo).

3. Scarica il certificato radice per Umbrella:
    1. Passare a Distribuzioni > Configurazione > Certificato radice.
    2. Selezionare Scarica certificato.
    3. Salvare il download come file `.cer`.
4. Modificare la configurazione e sostituire il segnaposto generico con la variabile corretta per Citrix MDM:

Variabile segnaposto generica	Nuova variabile
`Numero_seriale`	`${numeroseriale.dispositivo}`
`Indirizzo_MAC`*	`${indirizzo_MAC.dispositivo}`

*Si usa solo per il componente Clarity del CSC, non per il componente Umbrella.

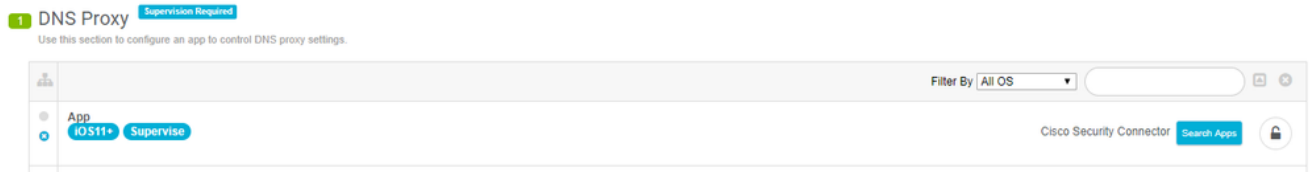
Quindi, completare i seguenti passaggi di MDM:

1. Configurare MDM per installare l'app CSC utilizzando Apple Business Manager (ABM) (in precedenza noto come VPP, Volume Purchase Program).
2. Caricare la configurazione Umbrella e/o Clarity modificata nei passaggi di preparazione.
3. Per importare il profilo, attenersi alla procedura descritta nella documentazione di Citrix.
4. Caricare il certificato del dispositivo per considerare attendibile l'Autorità di certificazione principale Umbrella.
5. Configurare i criteri per eseguire il push dei profili, di 1 CA e dell'app 1 CSC nei dispositivi richiesti.

MDM Lightspeed

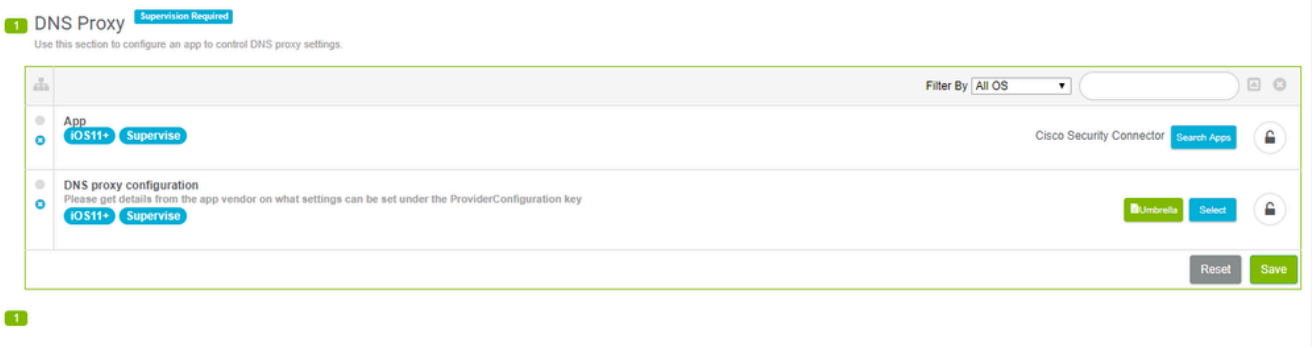
MDM Lightspeed supporta la configurazione basata su testo del proxy DNS iOS. A tale scopo, è possibile modificare il profilo MDM generico.

1. Scaricare il "file mobileconfig generico" e modificare l'estensione del file da .xml a .txt.
2. Aprire il file e modificare la stringa del numero di serie del segnaposto alla riga 58 in `%serial_number%`
3. In Velocità minima aggiungere Cisco Security Connection al profilo proxy DNS come illustrato

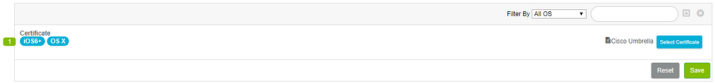


360019477192

4. Aggiungere il file mobileconfig generico modificato all'opzione di configurazione del proxy DNS sotto l'app.



360019477152

5. Infine, scaricare la Cisco Root CA da Umbrella e distribuirla in modalità Lightspeed per garantire pagine bloccate senza certificati. 

360019477132

I passi riportati di seguito si applicano alla distribuzione in tutti gli MDM. Attenersi innanzitutto alla procedura seguente.

Scuole JAMF

La distribuzione di CSC con JAMF Schools è diversa da JAMF. Iniziare con il profilo generico e vedere i passaggi nella documentazione di JAMF.

Di seguito è riportato un esempio di configurazione di dove selezionare e quale variabile utilizzare per il numero di 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. Crea un nuovo profilo in JAMF School.
   Per ulteriori informazioni, vedere la documentazione JAMF sui profili di dispositivo.
2. Utilizzare il payload del proxy DNS per configurare le impostazioni seguenti:
   1. Nel campo ID bundle app, immettere `com.cisco.ciscosecurity.app`.
   2. Nel campo ID bundle provider, immettere `com.cisco.ciscosecurity.app.CiscoUmbrella`.
3. Aggiungere il file XML creato nel passaggio 2 della documentazione JAMF alla configurazione del provider.

JAMF Precedente Alla 10.2.0

La distribuzione di CSC con JAMF richiede una modifica significativa del profilo. Per distribuire CSC con MDM JAMF, attenersi alla procedura descritta di seguito.

1. Assicurarsi che l'indirizzo e-mail dell'amministratore sia aggiunto al dashboard sotto l'opzione Impostazioni pagina Dispositivi mobili.
2. Aggiungere la CA radice Umbrella:
   1. Passare a Distribuzioni > Configurazione > Certificato radice.
   2. Selezionare Scarica certificato.
   3. Salvare il download come file cer.
   4. Specificare un nome per il certificato e selezionare Carica certificato.
   5. Caricare il file con estensione cer e lasciare vuoto il campo della password.
   6. Applica all'ambito dei dispositivi per il push out del certificato.
3. Scaricare il profilo generico dal dashboard Umbrella.
4. Se si utilizza JAMF Pro v.10.2.0 o versione successiva, è possibile ignorare questo passaggio. È possibile importare così com'è aggiungendo quanto segue:

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

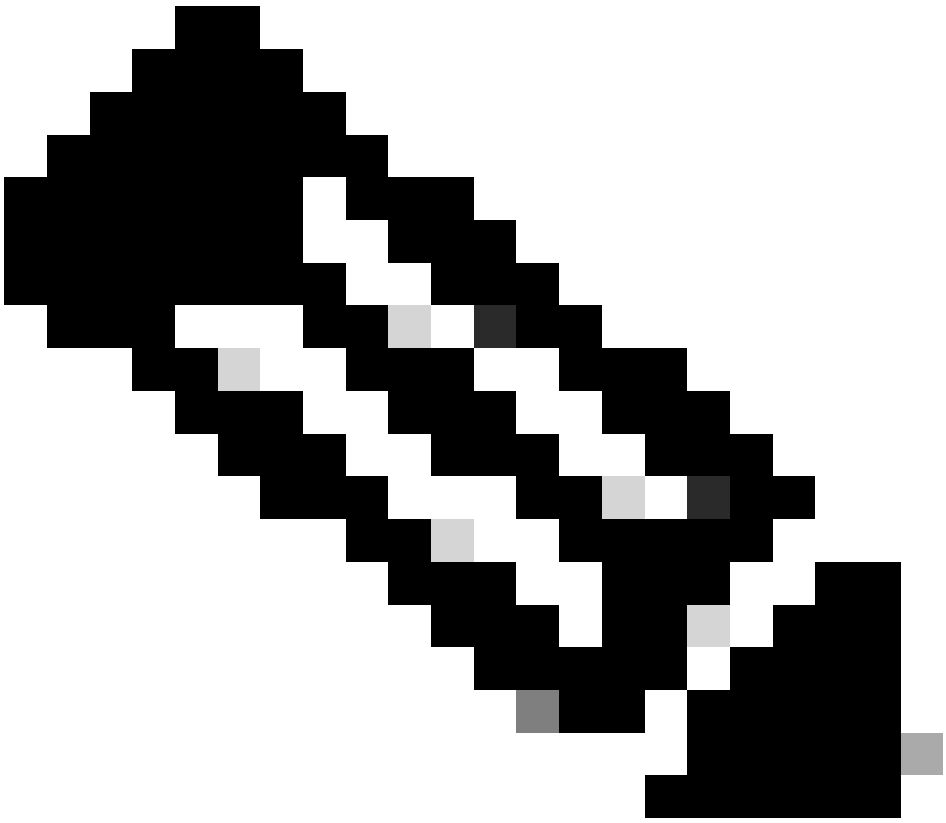
5. Se si utilizza una versione JAMF precedente alla v.10.2.0, modificare il profilo XML in modo esteso come illustrato in questo profilo di esempio. Non copiare questo esempio, in quanto

non funziona così com'è. Utilizzare solo la configurazione di download generica dal 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. Importa in JAMF:
    1. Nella finestra principale di configurazione MDM, fare clic su Nuovo per creare un nuovo profilo.



Nota: Deve essere un profilo separato e non deve essere utilizzato con il profilo certificato creato. Affinché l'app funzioni, questi due profili devono essere inviati al dispositivo separatamente.

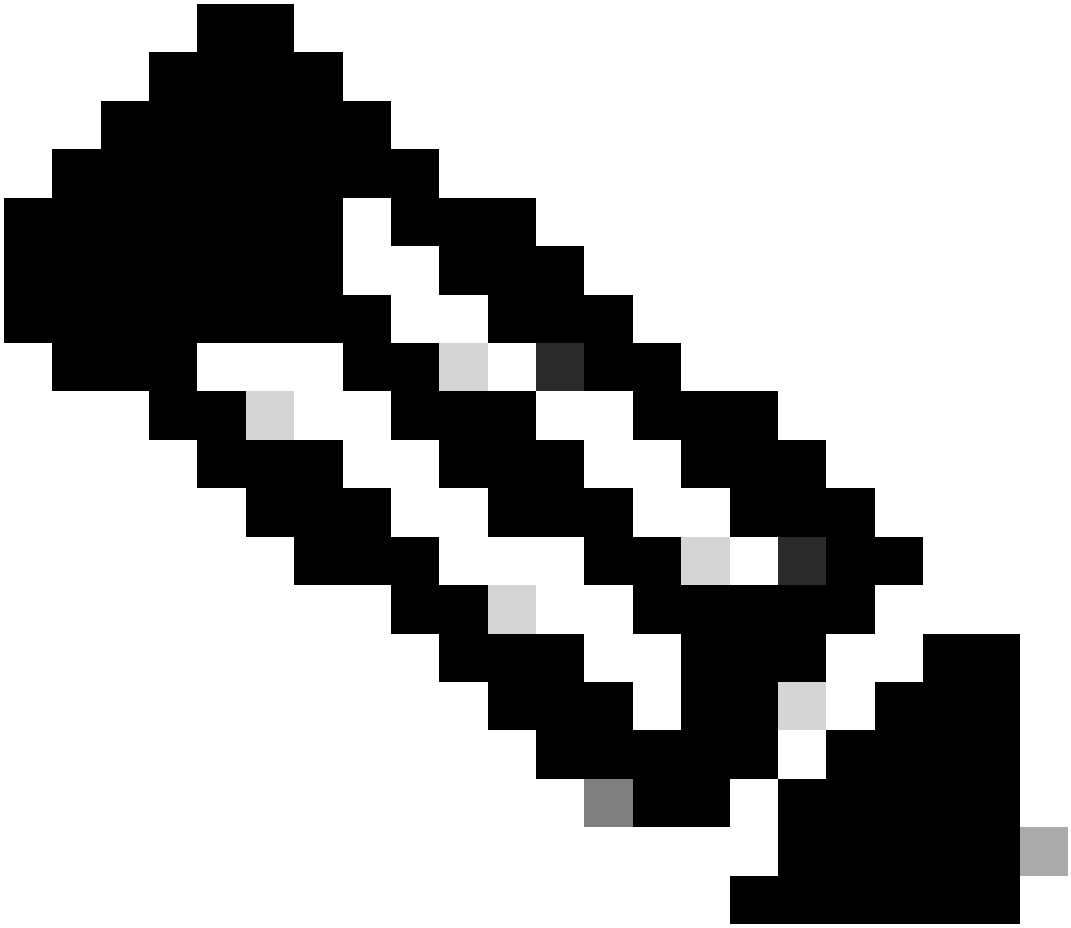
2. Assegnare un nome al profilo e passare al proxy DNS.
3. Sotto il proxy DNS, fare clic su Configura.
4. Impostare la configurazione proxy su Umbrella details:

    1. Nel campo ID bundle app, immettere `com.cisco.ciscosecurity.app`.
    2. Nel campo ID bundle provider, immettere: `com.cisco.ciscosecurity.app.CiscoUmbrella`.
    3. Incolla il contenuto XML modificato da Umbrella nella configurazione del provider XML.

5. Fare clic su Ambito e applicare all'ambito corretto dei dispositivi.

InTune

InTune viene aggiunto direttamente al dashboard Umbrella. Consulta la documentazione di Umbrella InTune per ulteriori informazioni.



> Nota: Clarity è un prodotto di Cisco AMP for Endpoints. Se non disponi di una licenza per questo prodotto, ignora la sezione relativa all'installazione.

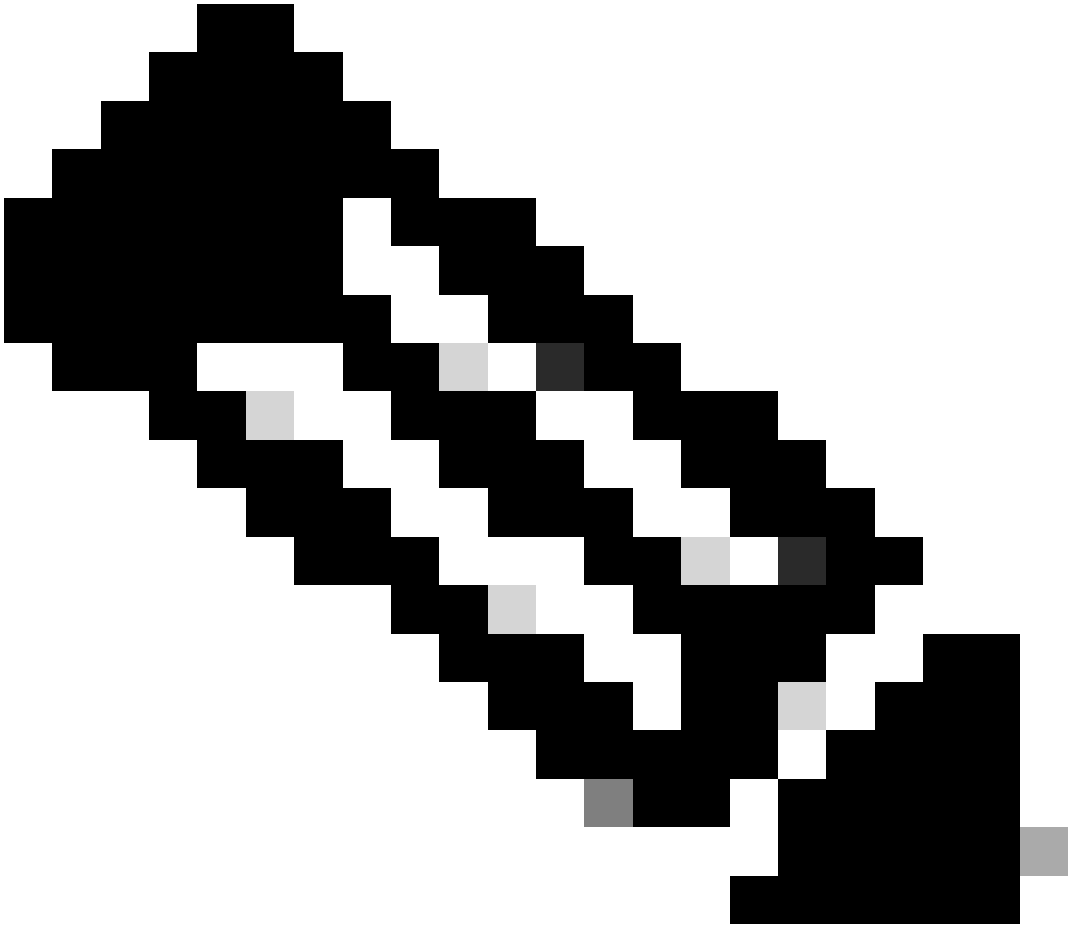
Mosyle

Il supporto per Mosyle è nel formato della configurazione del proxy DNS:

- Nel campo ID bundle app, immettere `com.cisco.ciscosecurity.app`.
- Nel campo ID bundle provider, immettere: `com.cisco.ciscosecurity.app.CiscoUmbrella`.

Aggiungere il contenuto all'interno di XML `<key>ProviderConfiguration</key>` al campo Model Provider Configuration:

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



> Nota: Per le impostazioni è necessario definire l'ambito dei dispositivi per la ricezione della configurazione e gli ambiti non vengono aggiunti per impostazione predefinita.

Protezione

Configurare in modo sicuro nella pagina Proxy DNS:

- Nel campo ID bundle app, immettere `com.cisco.ciscosecurity.app`

- Nel campo ID bundle provider , immettere `com.cisco.ciscosecurity.app.CiscoUmbrella`

Per configurare il file `.plist`, attenersi alla procedura seguente:

1. Iniziare con il modello iOS Common Config e modificare il file in un `.plist` con solo i commenti da `<dict>` a `</dict>` all'interno di `<key>ProviderConfiguration</key>`.
2. Sostituire la chiave `serialNumber` con la variabile `$serialnumber` definita da Security.
3. Il contenuto del file `.plist` può essere molto simile a questo esempio. Carica nella configurazione del 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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).