Implante o CSC para iOS em plataformas MDM adicionais

Contents

Introdução

Este documento descreve como implantar o Cisco Security Connector para iOS em plataformas adicionais de gerenciamento de dispositivos móveis.

Informações de Apoio

O Cisco Security Connector (CSC) para iOS é a proteção completa do Umbrella DNS para seu iPhone. Antes de usar este guia para implantações, leia a documentação de implantação do CSC. Seu dispositivo deve estar no modo supervisionado para usar o CSC.

Este documento resume o suporte de software de gerenciamento de dispositivo móvel (MDM) adicional para o CSC. Esses MDMs foram validados por uma implantação bem-sucedida, mas ainda não estão diretamente presentes no Painel.

Para verificar se um perfil existe em um dispositivo iOS:

1. Navegue até Configurações > Geral > Gerenciamento de dispositivos > [Nome do perfil MDM] > Mais detalhes.
2. Confirme se o tipo de perfil DNS Proxy está presente junto com estes detalhes:
    - Detalhes do aplicativo: `com.cisco.ciscosecurity.app`
    - Detalhes do pacote do provedor: `com.cisco.ciscosecurity.ciscoumbrella`

Leia mais sobre quais detalhes do perfil do iOS configurar no site MDM da Apple.

Todos os MDMs

Estas etapas se aplicam à implantação em todos os MDMs e devem ser concluídas primeiro:

1. Verifique se o endereço de e-mail do administrador foi adicionado ao painel na página "Configurações" da página "Dispositivos móveis".
2. Baixe o arquivo `Cisco_Umbrella_Root_CA.cer` para uso no dispositivo iOS. Este certificado permite páginas de bloqueio HTTPS sem erros. Para obter a CA raiz:
    1. Navegue até Implantações > Configuração > Certificado raiz.
    2. Selecione Download Certificate.
    3. Salve o download como um arquivo `.cer`.

Nuvem MobileIron

No momento, o download do MobileIron no painel suporta apenas a versão no local. A versão para nuvem usa variáveis de dispositivo diferentes do software local. A implantação é muito semelhante à implantada no local, com várias exceções. O MobileIron Core, dependendo da versão, pode exigir essa modificação.

Para implantar no MobileIron Cloud:

1. Verifique se o endereço de e-mail do administrador foi adicionado ao painel na página "Configurações" da página "Dispositivos móveis".
2. Baixe o perfil Mobile Iron no painel Umbrella.
3. Substitua estas variáveis:

Variável de espaço reservado genérica	Nova variável
`"$DEVICE_SN$"`	`${deviceSN}`
`"$DEVICE_MAC$"*`	`${deviceWifiMacAddress}`

*Isso é usado somente para o componente Clarity do CSC, não para o componente Umbrella. Se você não usar o Clarity, não há $DEVICE_MAC$ para substituir.

MDM de gerenciamento de endpoints da Citrix

Para implantar no Citrix, siga estas etapas de preparação no painel:

1. Verifique se o endereço de e-mail do administrador foi adicionado ao painel na página "Configurações" da página "Dispositivos móveis".
2. Faça o download da configuração MDM genérica do Umbrella (a AMP é configurada da mesma forma).
3. Baixar o certificado raiz do Umbrella:

    1. Navegue até Implantações > Configuração > Certificado raiz.
    2. Selecione Download Certificate.
    3. Salve o download como um arquivo `.cer`.
4. Modifique a configuração e substitua o espaço reservado genérico pela variável correta para o Citrix MDM:

Variável de espaço reservado genérica	Nova variável
`serial_number`	`${device.serialnumber}`
`Endereço_MAC*`	`${device.MAC_ADDRESS}`

*Isso é usado somente para o componente Clarity do CSC, não para o componente Umbrella.

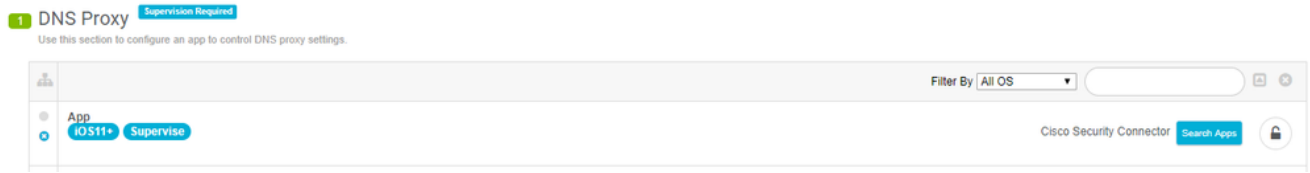
Em seguida, conclua estas etapas do MDM:

1. Configure o MDM para instalar o aplicativo CSC usando o Apple Business Manager (ABM) (anteriormente conhecido como VPP, Volume Purchase Program).
2. Carregue a configuração do Umbrella e/ou Clarity modificada nas etapas de preparação.
3. Use as etapas na documentação do Citrix para importar o perfil.
4. Carregue o certificado do dispositivo para confiar na Autoridade de Certificação Raiz do Guarda-Chuva.
5. Configure as políticas para enviar os perfis, 1 CA e 1 aplicativo CSC para o(s) dispositivo(s) necessário(s).

MDM Lightspeed

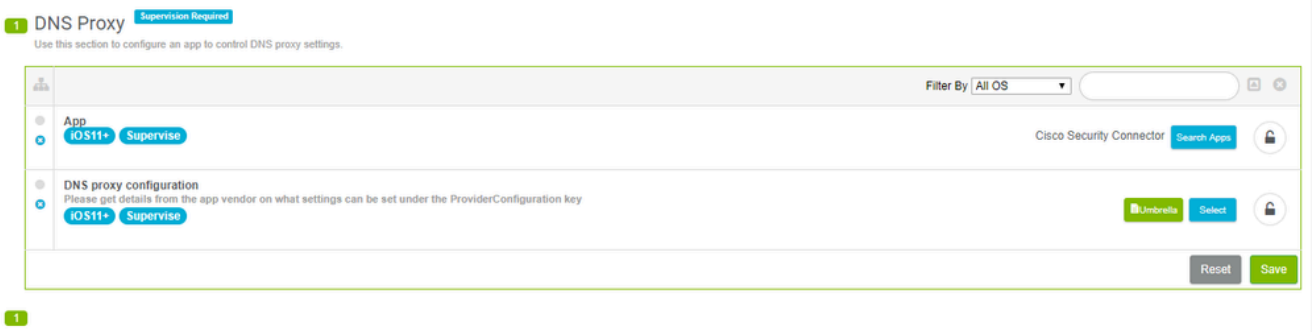
O Lightspeed MDM suporta configuração baseada em texto do proxy DNS do iOS. Isso pode ser feito modificando-se o perfil MDM genérico.

1. Faça o download do "arquivo mobileconfig genérico" e altere a extensão do arquivo de .xml para .txt.
2. Abra o arquivo e altere a sequência do número de série do espaço reservado na linha 58 para `%serial_number%`
3. No Lightspeed, adicione a conexão de segurança Cisco ao perfil de proxy DNS conforme mostrado



360019477192

4. Adicione o arquivo mobileconfig genérico modificado à opção de configuração de proxy DNS abaixo do aplicativo.



360019477152

5. Por fim, baixe a CA raiz da Cisco do Umbrella e implante-a no Lightspeed para garantir páginas de bloqueio sem certificado.

360019477132

Essas etapas se aplicam à implantação em todos os MDMs. Use essas etapas primeiro.

Escolas JAMF

A implantação do CSC com escolas JAMF é diferente do JAMF. Comece com o perfil genérico e consulte as etapas na documentação JAMF.

Aqui está um exemplo de configuração de onde selecionar e qual variável usar para o número de série:

```
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. Crie um novo perfil na Escola JAMF.
   Para obter mais informações, consulte a documentação JAMF em Perfis de dispositivo.
2. Use a carga do Proxy DNS para definir estas configurações:
   1. No campo ID do pacote de aplicativos, digite `com.cisco.ciscosecurity.app`.
   2. No campo ID do pacote do provedor, digite `com.cisco.ciscosecurity.app.CiscoUmbrella`.
3. Adicione o arquivo XML criado na etapa 2 da documentação JAMF à Configuração do provedor.

JAMF anterior a 10.2.0

A implantação do CSC com JAMF requer uma modificação significativa do perfil. Use estas etapas para implantar o CSC com JAMF MDM.

1. Verifique se o endereço de e-mail do administrador foi adicionado ao painel na página Configurações de dispositivos móveis opção.
2. Adicione a CA raiz do Umbrella:
   1. Navegue até Implantações **>** Configuração **>** Certificado raiz.
   2. Selecione Fazer download de certificado.
   3. Salve o download como um arquivo .cer.
   4. Forneça um nome para o certificado e selecione Carregar certificado.
   5. Carregue o .cer e deixe o campo de senha em branco.
   6. Aplique ao escopo de seus dispositivos para enviar este certificado.
3. Faça o download do perfil genérico do painel Umbrella.
4. Se estiver usando o JAMF Pro v.10.2.0 ou superior, você pode pular esta etapa. Você pode importar como está adicionando estes:

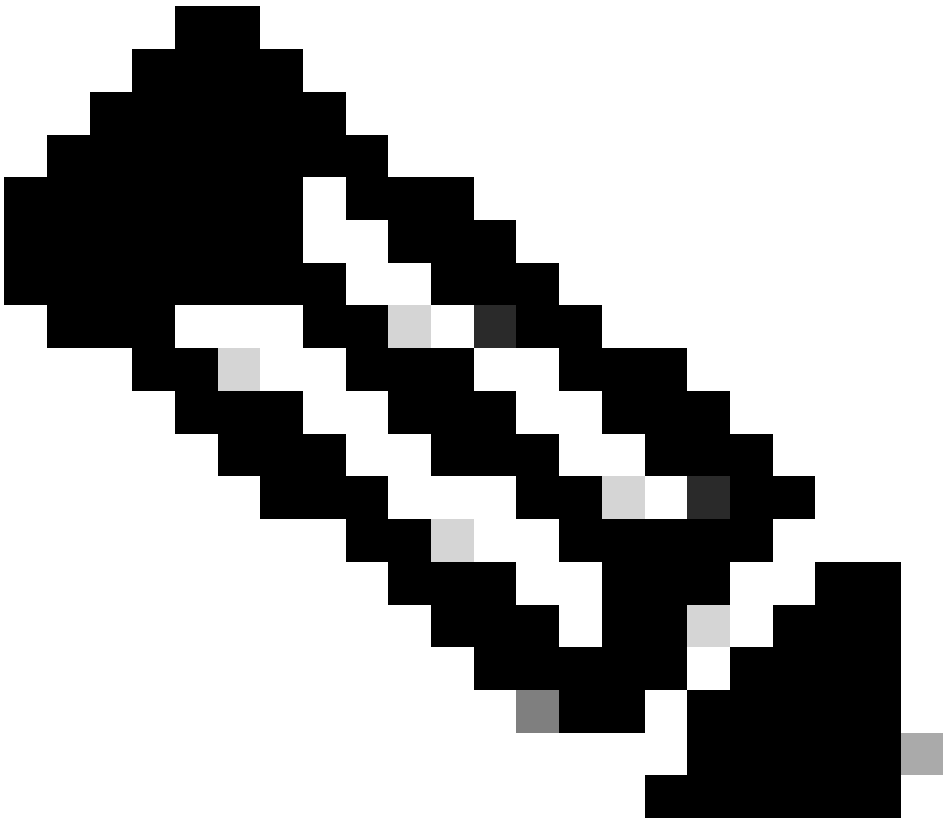
   ```
   <key>serialNumber</key>
   <string>$SERIALNUMBER</string>
   <key>label</key>
   <string>$DEVICENAME</string>
   ```

5. Se você estiver usando uma versão de JAMF anterior à v.10.2.0, edite o perfil XML extensivamente conforme mostrado neste perfil de exemplo. Não copie este exemplo, ele não está funcionando como está. Use apenas a configuração de download genérico do seu painel.

```
<?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 para JAMF:
    1. Na janela principal de configuração do MDM, clique em New para criar um novo perfil.

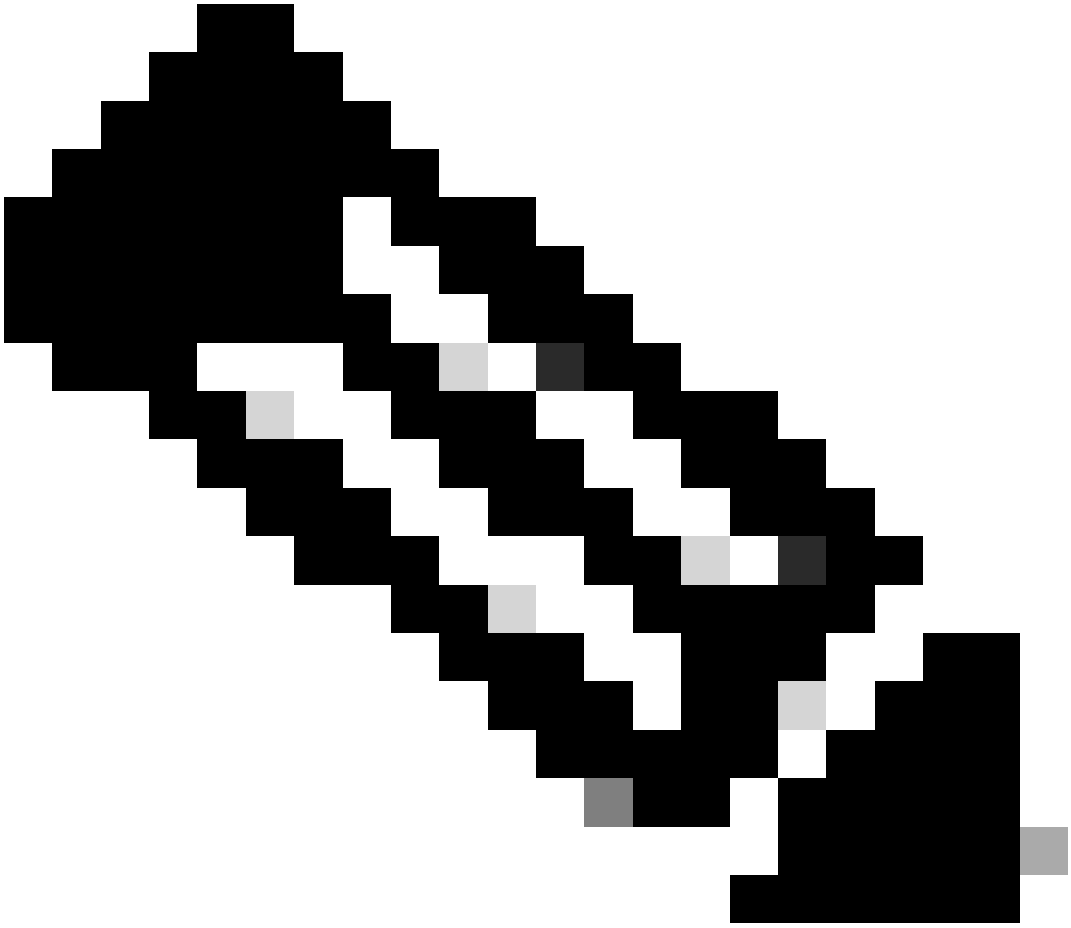


Note: Deve ser um perfil separado e não deve ser usado com o perfil de certificado criado. Para que o aplicativo funcione, esses dois perfis devem ser enviados para o dispositivo separadamente.

2. Nomeie o perfil e navegue até Proxy DNS.
3. No proxy DNS, clique em Configurar.
4. Defina a configuração do proxy como Detalhes do guarda-chuva:
    1. No campo ID do pacote de aplicativos, digite `com.cisco.ciscosecurity.app`.
    2. No campo ID do pacote do provedor, digite `com.cisco.ciscosecurity.app.CiscoUmbrella`.
    3. Colar o conteúdo XML editado do Umbrella na Configuração do provedor Seção XML.
5. Clique em Scope e aplique ao escopo apropriado dos dispositivos.

InTune

O InTune é adicionado diretamente ao painel Umbrella. Consulte a documentação do Umbrella InTune para obter mais informações.



Note: Clarity é um produto da Cisco AMP para endpoints. Se você não tiver uma licença para este produto, ignore a parte de instalação relacionada.

Mosyle

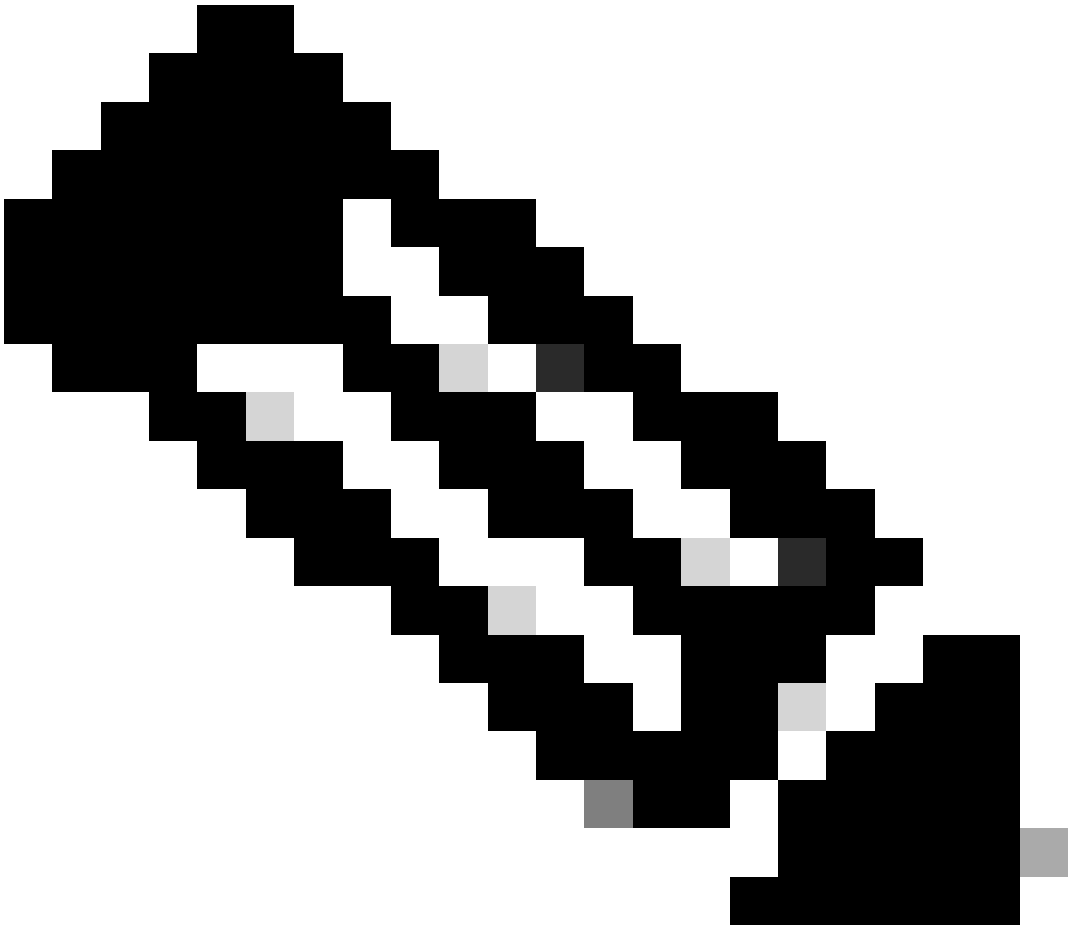
O suporte do Mosyle está na forma da configuração do Proxy DNS:

- No campo ID do pacote de aplicativos, digite `com.cisco.ciscosecurity.app`.
- No campo ID do pacote do provedor, digite `com.cisco.ciscosecurity.app.CiscoUmbrella`.

Adicione o conteúdo dentro do XML `<key>ProviderConfiguration</key>` ao campo Configuração do provedor Mosyle:

```
<dict>
```

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



Note: As configurações exigem que os dispositivos tenham escopo para receber a configuração, e os escopos não são adicionados por padrão.

Com segurança

Configurar com segurança na página de perfil do proxy DNS:

- No campo ID do pacote de aplicativos, digite `com.cisco.ciscosecurity.app`
- No campo ID do pacote do provedor, digite com.cisco.ciscosecurity.app.CiscoUmbrella

Siga estas etapas para configurar o arquivo `.plist`:

1. Comece com o modelo Configuração comum do iOS e edite o arquivo em um `.plist` somente com os comentários `<dict>` a `</dict>` dentro da `<key>ConfiguraçãoDoProvedor</key>`.
2. Substitua a chave `serialNumber` pela variável `$serialnumber conforme definido por Securly`.
3. O conteúdo do arquivo `.plist` pode ser muito semelhante a este exemplo. Carregue-o na configuração do 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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.