

# Solução de problemas do diretório corporativo

## "Host não encontrado"

### Contents

[Introdução](#)

[Informações de Apoio](#)

[Informações importantes](#)

[Cenário de trabalho](#)

[A URL do serviço telefônico está definida como Aplicativo:Cisco/CorporateDirectory e o telefone usa HTTP](#)

[Troubleshooting](#)

[Outros cenários em que ocorre o problema "Host não encontrado"](#)

### Introdução

Este documento descreve como solucionar problemas de "Host não encontrado" no recurso Corporate Directory dos telefones IP.

### Informações de Apoio

Informações importantes relevantes para este documento são:

- O diretório corporativo é um serviço de telefone IP padrão fornecido pela Cisco que é instalado automaticamente com o Cisco Unified Communications Manager (CUCM).
- As informações sobre a assinatura do telefone para os vários serviços de telefone são armazenadas no banco de dados nas tabelas telecasterservice, telecasterserviceparameter, telecastersubscribedparameter e telecastersubscribedservice.
- No telefone, quando você seleciona a opção Diretório corporativo, o telefone envia uma solicitação HTTP ou HTTPS para um dos servidores CUCM e é retornado como um objeto XML como uma resposta HTTP(S). Se HTTPS, isso também depende do telefone que se conecta ao serviço TVS para verificar o certificado para HTTPS. Em telefones que suportam midlets, isso pode ser implementado no midlet do telefone e afetado pela configuração [Provisionamento de serviços](#).

### Informações importantes

- Esclareça se o problema ocorre quando você acessa Diretórios ou Diretório corporativo.
- Como está definido o campo URL do serviço no serviço de diretório corporativo?
  - Se o URL estiver definido como Application:Cisco/CorporateDirectory, com base na versão do firmware do telefone, o telefone fará uma solicitação HTTP ou HTTPS.
  - Os telefones que usam o firmware versão 9.3.3 e posterior por padrão fazem uma solicitação HTTPS.
- Quando a URL do serviço está definida como Application:Cisco/CorporateDirectory, o telefone envia a solicitação HTTP(S) ao servidor que está primeiro em seu grupo CallManager (CM).
- Identifique a topologia de rede entre o telefone e o servidor para o qual a solicitação HTTP(S) é enviada.
- Preste atenção a firewalls, otimizadores de WAN, etc., no caminho que pode derrubar/difícultar o tráfego HTTP(S).
- Se o HTTPS estiver em uso, assegure a conectividade entre o telefone e o servidor TVS e que o TVS

esteja funcionando.

## Cenário de trabalho

Neste cenário, a URL do serviço telefônico é definida como Application:Cisco/CorporateDirectory e o telefone usa HTTPS.

Este exemplo mostra o arquivo de configuração do telefone com a URL correta.

```
<phoneService type="1" category="0">
<name>Corporate Directory</name>
<url>Application:Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

Nos registros do console do telefone, você pode verificar essas etapas.

### 1. O telefone usa o URL HTTPS.

```
7949 NOT 11:04:14.765155 CVM-appLaunchRequest: [thread=AWT-EventQueue-0]
[class=cip.app.G4ApplicationManager] Creating application module -
Corporate Directory
7950 ERR 11:04:14.825312 CVM-XsiAppData&colon;;getCdUrl:
[thread=appmgr MQThread]
[class=xxx.xxx.xx] Using HTTPS URL
```

### 2. O certificado Web Tomcat apresentado ao telefone a partir do servidor de diretórios não está disponível no telefone. Assim, o telefone tenta autenticar o certificado através do Trust Verification Service (TVS).

```
7989 ERR 11:04:15.038637 SECD: -HTTPS cert not in CTL, <10.106.111.100:8443>
7990 NOT 11:04:15.038714 SECD: -TVS service available, can attempt via TVS
```

### 3. O telefone procura primeiro no cache TVS e, se não for encontrado, entra em contato com o servidor TVS.

```
7995 NOT 11:04:15.039286 SECD: -TVS Certificate Authentication request
7996 NOT 11:04:15.039394 SECD: -No matching entry found at cache
```

### 4. Como a conexão com a TVS também é segura, uma autenticação de certificado é concluída e esta mensagem é impressa se for bem-sucedida.

```
8096 NOT 11:04:15.173585 SECD: -Successfully obtained a TLS connection
to the TVS server
```

### 5. O telefone agora envia uma solicitação para autenticar o certificado.

```
8159 NOT 11:04:15.219065 SECD: -Successfully sent the certificate Authentication
request to TVS server, bytes written : 962
8160 NOT 11:04:15.219141 SECD: -Done sending Certificate Validation request
8161 NOT 11:04:15.219218 SECD: -Authenticate Certificate : request sent to
```

TVS server - waiting for response

6. A resposta "0" da TVS significa que a autenticação foi bem-sucedida.

```
8172 NOT 11:04:15.220060 SECD: -Authentication Response received, status : 0
```

7. Essa mensagem é exibida e, em seguida, você vê a resposta.

```
8185 NOT 11:04:15.221043 SECD: -Authenticated the HTTPS conn via TVS
```

```
8198 NOT 11:04:15.296173 CVM-[truncated] Received
```

```
HTTP/1.1 200 OK^M
```

```
X-Frame-Options: SAMEORIGIN^M
```

```
Set-Cookie: JSESSIONID=660646D3655BB00734D3895606BCE76F;
```

```
Path=/ccmcip/; Secure; HttpOnly^M
```

```
Content-Type: text/xml;charset=utf-8^M
```

```
Content-Length: 966^M
```

```
Date: Tue, 30 Sep 2014 11:04:15 GMT^M
```

```
Server: ^M
```

```
^M
```

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>https://10.106.111.100:8443/ccmcip/xmldirectorylist.jsp</URL>
<InputItem><DisplayName>First Name</DisplayName>
<QueryStringParam>f</QueryStringParam><InputFlags>A</InputFlags>
<DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>
```

O processo de autenticação de certificado é semelhante ao discutido em [Phone Contacts Trust Verification Service for Unknown Certificate](#).

A partir das capturas de pacotes (PCAPs) coletadas na extremidade do telefone, você pode verificar a comunicação TVS com o uso desse filtro - tcp.port==2445.

Nos registros de TVS simultâneos:

1. Revise os rastreamentos em relação ao handshake do Transport Layer Security (TLS).
2. Em seguida, revise o despejo hexadecimal de entrada.

```
04:04:15.270 | debug ipAddrStr (Phone) 10.106.111.121
```

```
04:04:15.270 |<--debug
```

```
04:04:15.270 |-->debug
```

```
04:04:15.270 | debug 2:UNKNOWN:Incoming Phone Msg:
```

```
.
```

```
.
```

```
04:04:15.270 | debug
```

```
HEX_DUMP: Len = 960:
```

```
04:04:15.270 |<--debug
```

```
04:04:15.270 |-->debug
```

```
04:04:15.270 | debug 57 01 01 00 00 00 03 ea
```

```
.
<< o/p omitted >>
.
04:04:15.271 | debug MsgType : TVS_MSG_CERT_VERIFICATION_REQ
```

### 3. A TVS recupera os detalhes do emissor.

```
04:04:15.272 |-->CDefaultCertificateReader::GetIssuerName
04:04:15.272 | CDefaultCertificateReader::GetIssuerName got issuer name
04:04:15.272 |<--CDefaultCertificateReader::GetIssuerName
04:04:15.272 |-->debug
04:04:15.272 | debug tvsGetIssuerNameFromX509 - issuerName :
CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN and Length: 43
04:04:15.272 |<--debug
```

### 4. A TVS verifica o certificado.

```
04:04:15.272 | debug tvsGetSerialNumberFromX509 - serialNumber :
6F969D5B784D0448980F7557A90A6344 and Length: 16
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Looking up the certificate cache using Unique MAP ID :
6F969D5B784D0448980F7557A90A6344CN=cucm10;OU=TAC;O=Cisco;L=Blore;ST=KN;C=IN
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Certificate compare return =0
04:04:15.272 | debug CertificateDBCache::getCertificateInformation -
Certificate found and equal
```

### 5. A TVS envia a resposta para o telefone.

```
04:04:15.272 | debug 2:UNKNOWN:Sending CERT_VERIF_RES msg
04:04:15.272 | debug MsgType : TVS_MSG_CERT_VERIFICATION_RES
```

## A URL do serviço telefônico está definida como Aplicativo: Cisco/CorporateDirectory e o telefone usa HTTP

---

**Observação:** em vez do uso de uma versão anterior de firmware de telefone, o serviço e a URL de serviço segura foram codificados para a URL HTTP. No entanto, a mesma sequência de eventos é vista no firmware do telefone, que usa o HTTP por padrão.

---

O arquivo de configuração do telefone tem o URL correto.

```
<phoneService type="1" category="0">
<name>Corporate Directory</name>
<url>Application: Cisco/CorporateDirectory</url>
<vendor></vendor>
<version></version>
</phoneService>
```

Nos registros do console do telefone, você pode verificar essas etapas.

```

7250 NOT 11:44:49.981390 CVM-appLaunchRequest: [thread=AWT-EventQueue-0]
[class=cip.app.G4ApplicationManager] Creating application module -
Corporate Directory/-838075552
7254 NOT 11:44:50.061552 CVM-_HTTPMakeRequest1: Processing Non-HTTPS URL
7256 NOT 11:44:50.061812 CVM-_HTTPMakeRequest1() theHostname: 10.106.111.100:8080

```

```

7265 NOT 11:44:50.233788 CVM-[truncated] Received
HTTP/1.1 200 OK^M
X-Frame-Options: SAMEORIGIN^M
Set-Cookie: JSESSIONID=85078CC96EE59CA822CD607DDAB28C91;
Path=/ccmcip/; HttpOnly^M
Content-Type: text/xml;charset=utf-8^M
Content-Length: 965^M
Date: Tue, 30 Sep 2014 11:44:50 GMT^M
Server: ^M
^M
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><CiscoIPPhoneInput>
<Title>Directory Search</Title><Prompt>Enter search criteria</Prompt><SoftKeyItem>
<Name>Search</Name><Position>1</Position><URL>SoftKey:Submit</URL></SoftKeyItem>
<SoftKeyItem><Name>&lt;&lt;</Name><Position>2</Position><URL>SoftKey:&lt;&lt;</URL>
</SoftKeyItem><SoftKeyItem><Name>Cancel</Name><Position>3</Position>
<URL>SoftKey:Cancel</URL></SoftKeyItem>
<URL>http://10.106.111.100:8080/ccmcip/xmldirectorylist.jsp</URL><InputItem>
<DisplayName>First Name</DisplayName><QueryStringParam>f</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></InputItem><InputItem>
<DisplayName>Number</D

```

Nas capturas de pacotes, você verá uma solicitação HTTP GET e uma RESPOSTA bem-sucedida. Este é o PCAP do CUCM:

No.	Time	Source	Destination	Protocol	Length	Info
87	2015-01-23 09:04:10.358018000	64.103.236.200	10.106.111.99	HTTP	472	GET /ccmcip/xmldirectoryinput.jsp?name=SEP0021CC899172 HTTP/1.1
89	2015-01-23 09:04:10.948677000	10.106.111.99	64.103.236.200	HTTP/XML	1173	HTTP/1.1 200 OK

## Troubleshooting

Antes de solucionar o problema, reúna os detalhes listados anteriormente:

Logs a serem coletados, se necessário

- Capturas de pacotes simultâneas do telefone IP e do servidor CUCM (o servidor que está primeiro em seu grupo CM para onde a solicitação HTTP(S) seria enviada).
- Registros do console do telefone IP.
- Registros do Cisco TVS (detalhado).

Quando você define os logs de TVS como detalhado, o serviço precisa ser reiniciado para que as alterações no nível de rastreamento ocorram. Consulte o bug da Cisco ID [CSCuq2327](#) para obter informações sobre como notificar que é necessário reiniciar o serviço quando os níveis de log são alterados.

Conclua estas etapas para isolar o problema:

Etapa 1.

Crie um serviço de teste com estes detalhes:

Service Name : <Any Name>  
Service URL : http://<CUCM\_IP\_Address>:8080/ccmcip/xmldirectoryinput.jsp  
Secure-Service URL : http://<CUCM\_IP\_Address>:8080/ccmcip/xmldirectoryinput.jsp  
Service Category : XML Service  
Service Type : Directories  
Enable : CHECK  
Enterprise Subscription : DO NOT CHECK

Agora, assine este serviço para um dos telefones afetados:

- a. Vá para a página de configuração do dispositivo.
- b. Selecione **Subscribe/Unsubscribe Services** em Related Links.
- c. **Assine** o serviço de teste que você criou.
- d. **Salve**, aplique a configuração e reinicie o telefone.
  - i. O que você fez, independentemente da versão FW do telefone, que determina se deve usar o URL HTTP ou HTTPS, é forçá-lo a usar o URL HTTP.
  - ii. Acesse o serviço de diretório corporativo no telefone.
  - iii. Se isso não funcionar, colete os registros mencionados anteriormente e compare-os com o cenário de trabalho mencionado na seção Cenário de trabalho e identifique onde o desvio está.
  - iv. Se funcionar, você pelo menos confirmou que da perspectiva do serviço de telefone IP CUCM não há problemas.
  - v. Nesse estágio, o problema é mais provável com os telefones que usam o URL HTTPS.
  - vi. Agora, escolha um telefone que não funcione e vá para a próxima etapa.

Quando essa alteração funcionar, você precisará decidir se não há problema em deixar a configuração com a solicitação/resposta do diretório corporativo que funciona por HTTP em vez de HTTPS. A comunicação HTTPS não funciona devido a um dos motivos discutidos a seguir.

Etapa 2.

Colete os registros mencionados anteriormente, compare-os com o cenário de trabalho mencionado na seção Cenário de trabalho e identifique onde o desvio está.

Pode ser um destes problemas:

- a. O telefone não consegue entrar em contato com o servidor TVS.
  - i. No PCAPS, verifique a comunicação na porta 2445.
  - ii. Certifique-se de que nenhum dos dispositivos de rede no caminho bloqueie essa porta.
- b. O telefone entra em contato com o servidor TVS, mas o handshake TLS falha.

Estas linhas podem ser impressas nos registros do console do telefone:

```
5007: NOT 10:25:10.060663 SECD: clpSetupSsl: Trying to connect to IPV4,  
IP: 192.168.136.6, Port : 2445  
5008: NOT 10:25:10.062376 SECD: clpSetupSsl: TCP connect() waiting,  
<192.168.136.6> c:14 s:15 port: 2445  
5009: NOT 10:25:10.063483 SECD: clpSetupSsl: TCP connected,  
<192.168.136.6> c:14 s:15  
5010: NOT 10:25:10.064376 SECD: clpSetupSsl: start SSL/TLS handshake,  
<192.168.136.6> c:14 s:15
```

```
5011: ERR 10:25:10.068387 SECD: EROR:clpState: SSL3 alert
      read:fatal:handshake failure:<192.168.136.6>
5012: ERR 10:25:10.069449 SECD: EROR:clpState: SSL_connect:failed in SSLv3
      read server hello A:<192.168.136.6>
5013: ERR 10:25:10.075656 SECD: EROR:clpSetupSsl: ** SSL handshake failed,
      <192.168.136.6> c:14 s:15
5014: ERR 10:25:10.076664 SECD: EROR:clpSetupSsl: SSL/TLS handshake failed,
      <192.168.136.6> c:14 s:15
5015: ERR 10:25:10.077808 SECD: EROR:clpSetupSsl: SSL/TLS setup failed,
      <192.168.136.6> c:14 s:15
5016: ERR 10:25:10.078771 SECD: EROR:clpSndStatus: SSL CLNT ERR,
      srvr<192.168.136.6>
```

Consulte o bug da Cisco ID [CSCua65618](#) para obter mais informações.

- c. O telefone entra em contato com os servidores TVS, e o handshake TLS é bem-sucedido, mas a TVS não consegue verificar o assinante do certificado que o telefone solicitou para autenticar.

Os trechos de registros da TVS estão listados aqui:

O telefone entra em contato com a TVS.

```
05:54:47.779 | debug 7:UNKNOWN:Got a new ph conn 10.106.111.121 on 10, Total Acc = 6..
.
.
05:54:47.835 | debug      MsgType                : TVS_MSG_CERT_VERIFICATION_REQ
```

A TVS obtém o nome do emissor.

```
05:54:47.836 |-->CDefaultCertificateReader::GetIssuerName
05:54:47.836 | CDefaultCertificateReader::GetIssuerName got issuer name
05:54:47.836 |<--CDefaultCertificateReader::GetIssuerName
05:54:47.836 |-->debug
05:54:47.836 | debug tvsGetIssuerNameFromX509 - issuerName :
      CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN and Length: 49
```

Ele pesquisa o certificado, mas não o encontra.

```
05:54:47.836 | debug CertificateCTLCache::getCertificateInformation
      - Looking up the certificate cache using Unique MAP ID :
      62E09123B09A61D20E77BE5BF5A82CD4CN=cucmpub9;OU=TAC;O=Cisco;L=Bangalore;ST=KN;C=IN
05:54:47.836 |<--debug
05:54:47.836 |-->debug
05:54:47.836 | debug ERROR:CertificateCTLCache::getCertificateInformation
      - Cannot find the certificate in the cache
05:54:47.836 |<--debug
05:54:47.836 |-->debug
05:54:47.836 | debug getCertificateInformation(cert) : certificate not found
```

d. O tráfego HTTPS é bloqueado/descartado em algum lugar da rede.

Obtenha PCAPs simultâneos do telefone e do servidor CUCM para verificar a comunicação.

## **Outros cenários em que ocorre o problema "Host não encontrado"**

1. O servidor CUCM é definido pelo nome do host junto com problemas na resolução de nomes.
2. A lista de servidores TVS está vazia no telefone quando ele baixa o arquivo xmldefault.cnf.xml. (Na versão 8.6.2, o arquivo de configuração padrão não tem a entrada TVS nele devido ao bug da Cisco ID [CSCti64589](#).)
3. O telefone não pode usar a entrada TVS no arquivo de configuração porque ele fez o download do arquivo xmldefault.cnf.xml. Consulte o bug da Cisco ID [CSCuq3297](#) - Telefone para analisar informações de TVS do arquivo de configuração padrão.
4. O diretório corporativo não funciona após uma atualização do CUCM porque o firmware do telefone é atualizado para uma versão posterior, que eventualmente altera o comportamento do uso de HTTPS por padrão.

## 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.