

# 社内ディレクトリ"; ホストが見つからない"; 問題のトラブルシューティング

## 内容

---

[はじめに](#)

[背景説明](#)

[重要な情報](#)

[正常動作シナリオ](#)

[電話サービスのURLがApplication: Cisco/CorporateDirectoryに設定され、電話がHTTPを使用する](#)

[トラブルシュート](#)

[「ホストが見つかりません」問題が発生するその他のシナリオ](#)

---

## はじめに

このドキュメントでは、IP Phoneの社内ディレクトリ機能の「ホストが見つかりません」の問題をトラブルシューティングする方法について説明します。

## 背景説明

このドキュメントに関連する重要な情報は次のとおりです。

- 社内ディレクトリは、Cisco Unified Communications Manager(CUCM)とともに自動的にインストールされる、シスコが提供するデフォルトのIP Phoneサービスです。
- さまざまな電話サービスへの電話サブスクリプションに関する情報は、telecasterservice、telecasterserviceparameter、telecastersubscribedparameter、telecastersubscribedserviceテーブルのデータベースに保存されます。
- 電話機で、オプションの社内ディレクトリを選択すると、電話機はHTTPまたはHTTPS要求をCUCMサーバの1つに送信し、HTTP(S)応答としてXMLオブジェクトとして返されます。HTTPSの場合、これはTVSサービスに接続している電話機がHTTPSの証明書を確認するかどうかによっても異なります。MIDletをサポートする電話機では、この機能を電話機のMIDletに実装でき、[サービスプロビジョニング](#)設定の影響を受けます。

## 重要な情報

- ディレクトリまたは社内ディレクトリにアクセスする際に問題が発生するかどうかを明確にします。
- Corporate Directoryサービスの下で設定されるService URフィールドは何ですか。
  - URLがApplication: Cisco/CorporateDirectoryに設定されている場合、電話機のファームウェアバージョンに基づいて、電話機はHTTPまたはHTTPS要求を行います。
  - デフォルトでファームウェアバージョン9.3.3以降を使用する電話機は、HTTPS要求を

行います。

- サービスURLがApplication:Cisco/CorporateDirectoryに設定されている場合、電話機はCallManager(CM)グループの最初にあるサーバにHTTP(S)要求を送信します。
- HTTP(S)要求の送信先となる電話機とサーバの間のネットワークポロジを特定します。
- HTTP(S)トラフィックをドロップまたは妨害する可能性のあるパス内のファイアウォール、WANオプティマイザなどに注意してください。
- HTTPSを使用している場合は、電話とTVSサーバ間の接続と、TVSが機能していることを確認します。

## 正常動作シナリオ

このシナリオでは、電話サービスのURLはApplication:Cisco/CorporateDirectoryに設定され、電話はHTTPSを使用します。

次の例は、正しいURLを持つ電話機のコンフィギュレーションファイルを示しています。

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

電話機のコンソールログから、次の手順を確認できます。

### 1. 電話機はHTTPS URLを使用します。

```
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. ディレクトリサーバから電話機に提示されたTomcat Web証明書は、電話機では使用できません。そのため、電話機はTrust Verification Service(TVS)を介して証明書の認証を試みます。

```
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. 電話機は最初にTVSキャッシュを検索し、見つからない場合はTVSサーバに接続します。

```
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. TVSへの接続も安全であるため、証明書認証が完了し、成功した場合はこのメッセージが表

示されません。

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

#### 5. 電話機は、証明書の認証要求を送信します。

```
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. TVSからの応答「0」は、認証が成功したことを意味します。

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

#### 7. 次のメッセージが表示され、応答が表示されます。

```
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>
<FormItem><DisplayName>First Name</DisplayName>
<QueryStringParam>f</QueryStringParam><InputFlags>A</InputFlags>
<DefaultValue></DefaultValue></FormItem><FormItem>
<DisplayName>Last Name</DisplayName><QueryStringParam>l</QueryStringParam>
<InputFlags>A</InputFlags><DefaultValue></DefaultValue></FormItem><FormItem>
<DisplayName>
```

証明書認証プロセスは、「[不明な証明書に対する電話機の連絡先の信頼検証サービス](#)」で説明したものと似ています。

電話側で収集されたパケットキャプチャ(PCAP)から、このフィルタtcp.port==2445を使用してTVS通信を確認できます。

同時TVSログで、次の操作を行います。

#### 1. Transport Layer Security(TLS)ハンドシェイクに関してトレースを確認します。

## 2. 次に、受信した16進数ダンプを確認します。

```
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. TVSは発行者の詳細を取得します。

```
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=Bllore;ST=KN;C=IN and Length: 43
04:04:15.272 |<--debug
```

## 4. TVSが証明書を確認します。


```
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=Bllore;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. TVSが電話に応答を送信します。


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

## 電話サービスのURLがApplication: Cisco/CorporateDirectoryに設定され、電話がHTTPを使用する

---

 注：以前の電話ファームウェアバージョンを使用する代わりに、サービスおよびセキュアサービスのURLがHTTP URLにハードコードされました。ただし、デフォルトでHTTPを使用

---

 する電話機のファームウェアでも同じ順序でイベントが発生します。

電話機の設定ファイルに正しいURLが含まれている。

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

電話機のコンソールログから、次の手順を確認できます。

```
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
```

パケットキャプチャから、HTTP GET要求と正常なRESPONSEが表示されます。これはCUCMからのPCAPです。

No.	Time	Source	Destination	Protocol	Length	Info
87	2015-01-23 09:04:10.358018000	64.103.236.206	10.106.111.99	HTTP	472	GET /ccmcip/xmldirectoryinput.jsp?name=SEP0021CC699172 HTTP/1.1
89	2015-01-23 09:04:10.368077000	10.106.111.99	64.103.236.206	HTTP/XML	1173	HTTP/1.1 200 OK

# トラブルシューティング

トラブルシューティングを行う前に、前述の問題の詳細を収集します。

必要に応じて収集するログ

- IP電話とCUCMサーバ(HTTP(S)要求の送信先となるCMグループの最初のサーバ)からの同時パケットキャプチャ。
- IP Phoneコンソールログ。
- Cisco TVSログ ( 詳細 )

TVSログをdetailedに設定すると、トレースレベルの変更を実行するためにサービスを再起動する必要があります。ログレベルが変更されたときにサービスの再起動が必要であることを通知する機能拡張については、Cisco Bug ID [CSCuq22327](#)を参照してください。

次の手順を実行して、この問題を切り分けます。

ステップ 1 :

次の詳細情報を使用してテストサービスを作成します。

```
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
```

ここで、このサービスを該当する電話機のいずれかに登録します。

- a. デバイス設定ページに移動します。
- b. Related Linksの下にあるSubscribe/Unsubscribe Servicesを選択します。
- c. 作成したテストサービスを登録します。
- d. 保存、設定の適用、および電話機のリセットを行います。
  - i. 電話のFWバージョンに関係なく、HTTPまたはHTTPS URLを使用するかどうかを決定する操作によって、HTTP URLを強制的に使用します。
  - ii. 電話機で社内ディレクトリサービスにアクセスします。
  - iii. 正常に動作しない場合は、前述のログを収集し、「動作シナリオ」セクションで説明した動作シナリオと比較して、偏差の場所を特定します。
  - iv. 動作する場合は、少なくともCUCM IP Phoneサービスの観点から問題がないことを確認しています。
  - v. この段階では、問題はHTTPS URLを使用する電話機で発生する可能性が最も高いです。
  - vi. ここで、動作しない電話を選択し、次の手順に進みます。

この変更に対応する場合は、HTTPSではなくHTTPで動作する社内ディレクトリ要求/応答を使用

して設定を終了しても問題ないかどうかを判断する必要があります。次に説明する理由の1つが原因で、HTTPS通信が機能しません。

ステップ 2 :

前述のログを収集し、「作業シナリオ」セクションで説明した作業シナリオと比較して、偏差の場所を特定します。

次のいずれかの問題が考えられます。

- a. 電話機がTVSサーバに接続できません。
  - i. PCAPSで、ポート2445の通信を確認します。
  - ii. パス内のどのネットワークデバイスもこのポートをブロックしていないことを確認します。
- b. 電話機はTVSサーバに接続しますが、TLSハンドシェイクが失敗します。

次の行は、電話機のコンソールログに出力できます。

```
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>
```

詳細については、Cisco Bug ID [CSCua65618](#)を参照してください。

- c. 電話がTVSサーバに接続し、TLSハンドシェイクは成功しますが、TVSは電話が認証を要求した証明書の署名者を確認できません。

TVSログのスニペットを次に示します。

電話機がTVSに接続されます。

```
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
```

TVSは発行者名を取得します。

```
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
```

証明書を検索しますが、見つかりません。

```
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. HTTPSトラフィックは、ネットワークのどこかでブロックまたはドロップされます。

通信を確認するために、電話機とCUCMサーバから同時PCAPを取得します。

## 「ホストが見つかりません」問題が発生するその他のシナリオ

1. CUCMサーバは、名前解決の問題とともにホスト名によって定義されます。
2. 電話機がxmldefault.cnf.xmlファイルをダウンロードするとき、TVSサーバリストは空です。(バージョン8.6.2では、Cisco Bug ID [CSCTi64589](#)が原因で、デフォルトのコンフィギュレーションファイルにTVSエントリが含まれていません)。
3. 電話機は、xmldefault.cnf.xmlファイルをダウンロードしたため、設定ファイルのTVSエントリを使用できません。Cisco Bug ID [CSCuq33297](#) : デフォルトのコンフィギュレーションファイルからTVS情報を解析する電話機を参照してください。
4. CUCMのアップグレード後に社内ディレクトリが機能しません。これは、電話機のファームウェアが新しいバージョンにアップグレードされ、その結果、デフォルトでHTTPSを使用する動作が変更されるためです。



## 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。