

Resolva os problemas mais comuns da margem de colaboração

Contents

[Introdução](#)

[Informações de Apoio](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problemas de login](#)

[O Jabber não consegue iniciar sessão por MRA](#)

[1. Registro de Serviço de Borda de Colaboração \(SRV\) Não Criado e/ou Porta 8443 Inalcançável](#)

[2. Certificado Inaceitável ou Indisponível no VCS Expressway](#)

[3. Nenhum Servidor UDS Encontrado na Configuração de Borda](#)

[4. Os logs do Expressway-C mostram este erro: Detalhes de XCP_JABBERD=Não é possível conectar ao host '%IP%', porta 7400:\(111\) Conexão recusada](#)

[5. O nome de host/nome de domínio do servidor Expressway-E não corresponde ao que está configurado no SRV_collab-edge](#)

[6. Não é possível fazer logon devido a uma assinatura atual do WebEx Connect](#)

[7. O servidor Expressway-C exibe a mensagem de erro: "Configurado, mas com erros. Servidor de provisionamento: aguardando informações do servidor de passagem."](#)

[8. Microsoft DirectAccess Instalado](#)

[9. Falhas nas Pesquisas de DNS Reverso do Expressway](#)

[Problemas de registro](#)

[Softphone não pode se registrar, método SIP/2.0 405 não permitido](#)

[Softphone não pode registrar, Reason="Domínio desconhecido"](#)

[Softphone não pode se registrar, motivo "contagem regressiva ociosa expirou"](#)

[O MRA falha devido ao proxy do telefone configurado no firmware](#)

[Problemas relacionados a chamadas](#)

[Nenhuma Mídia ao Chamar por MRA](#)

[Sem Toque de Retorno ao Chamar sobre MRA para PSTN](#)

[Problemas de CUCM e IM&P](#)

[Erro ASCII que impede a adição de CUCM](#)

[Falhas de TLS de saída no 5061 do Expressway-C para CUCM em implantações seguras](#)

[Servidor IM&P Não Adicionado e Erros Encontrados](#)

[Questões diversas](#)

[O status do correio de voz no cliente Jabber mostra "Não conectado"](#)

[As fotos de contato não aparecem em clientes Jabber através do Expressways](#)

[Os clientes Jabber são solicitados a aceitar o certificado Expressway-E durante o login](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como solucionar os problemas mais comuns do Collaboration Edge que você enfrenta durante a fase de implantação.

Informações de Apoio

O acesso remoto e móvel (MRA) é uma solução de implantação para o recurso Virtual Private Network-less (VPN) Jabber. Essa solução permite que os usuários finais se conectem aos recursos internos da empresa de qualquer lugar do mundo. Este guia foi escrito para dar aos engenheiros que solucionam problemas da solução Collaboration Edge a capacidade de identificar e resolver rapidamente os problemas mais comuns que você enfrenta durante a fase de implantação.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM)
- Núcleo do Cisco Expressway
- Cisco Expressway Edge
- Mensagens instantâneas e presença (IM&P) da Cisco
- Cisco Jabber para Windows
- Cisco Jabber para MAC
- Cisco Jabber para Android
- Cisco Jabber para iOS®
- Certificados de segurança
- Domain Name System (DNS)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Expressway Versão X8.1.1 ou posterior
- CUCM Versão 9.1(2)SU1 ou posterior e IM&P Versão 9.1(1) ou posterior
- Cisco Jabber versão 9.7 ou posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Problemas de login

O Jabber não consegue iniciar sessão por MRA

Esse sintoma pode ser causado por uma grande variedade de problemas, alguns dos quais estão descritos aqui.

1. Registro de Serviço de Borda de Colaboração (SRV) Não Criado e/ou Porta 8443 Inalcançável

Para que um cliente Jabber possa fazer login com sucesso com o MRA, um registro SRV de borda de colaboração específico deve ser criado e acessível externamente. Quando um cliente Jabber é iniciado inicialmente, ele faz consultas DNS SRV:

1. `_cisco-uds`: este registro SRV é usado para determinar se um servidor CUCM está disponível.
2. `_cuplogin`: este registro SRV é usado para determinar se um servidor IM&P está disponível.
3. `_collab-edge`: este registro SRV é usado para determinar se a MRA está disponível.

Se o cliente Jabber for iniciado e não receber uma resposta SRV para `_cisco-uds` e `_cuplogin` e não receber uma resposta para `_collab-edge`, ele usará essa resposta para tentar entrar em contato com o Expressway-E listado na resposta SRV.

O registro SRV `_collab-edge` aponta para o nome de domínio totalmente qualificado (FQDN) do Expressway-E com a porta 8443. Se o SRV `_collab-edge` não for criado, não estiver disponível externamente ou se estiver disponível, mas a porta 8443 não estiver acessível, o cliente Jabber falhará ao fazer login.

Você pode confirmar se o registro SRV `_collab-edge` pode ser resolvido e se a porta TCP 8443 pode ser alcançada com o verificador SRV no [Collaboration Solutions Analyzer \(CSA\)](#).

Se a porta 8443 não estiver acessível, isso pode ocorrer porque um dispositivo de segurança (Firewall) bloqueia a porta ou uma configuração incorreta do Gateway Padrão (GW) ou das rotas estáticas no Exp-E.

2. Certificado Inaceitável ou Indisponível no VCS Expressway

Depois que o cliente Jabber recebe uma resposta para `_collab-edge`, ele entra em contato com o Expressway com Transport Layer Security (TLS) pela porta 8443 para tentar recuperar o certificado do Expressway para configurar o TLS para comunicação entre o cliente Jabber e o Expressway.

Se o Expressway não tiver um certificado assinado válido que contenha o FQDN ou o domínio do Expressway, isso falhará e o cliente Jabber falhará ao fazer login.

Se esse problema ocorrer, use a ferramenta CSR (Certificate Signing Request, Solicitação de assinatura de certificado) no Expressway, que inclui automaticamente o FQDN do Expressway como SAN (Subject Alternative Name, Nome alternativo do assunto).

 Observação: o MRA requer comunicação segura entre o Expressway-C e o Expressway-E e entre o Expressway-E e os endpoints externos.

A próxima tabela com os requisitos de certificado do Expressway por recurso pode ser encontrada no [Guia de implantação de MRA](#):

Table 1. CSR Alternative Name Element and Unified Communications Features

Add These Items as Subject Alternative Names	When Generating a CSR for These Purposes			
	Mobile and Remote Sccess	Jabber guest	XMPP Federation	Business to Business Calls
Unified CM registrations domains (despite their name, these have more in common with service discovery domains than with Unified CM Unified CM SIP registration domains)	Required on Expressway-E only	–	–	–
XMPP federation domains	–	–	Required on Expressway-E only	–
IM and Presence Service chat node aliases (federated group chat)	–	–	Required	–
Unified CM phone security profile names	Required on Expressway-C only	–	–	–
(Clustered systems only) Expressway cluster name	Required on Expressway-C only	Required on Expressway-C only	Required on Expressway-C only	–

3. Nenhum Servidor UDS Encontrado na Configuração de Borda

Depois que o cliente Jabber estabelece com êxito uma conexão segura com o Expressway-E, ele solicita sua configuração de borda (get_edge_config). Esta configuração de borda contém os registros SRV para _cuplogin e _cisco-uds. Se os registros SRV _cisco-uds não forem retornados na configuração de borda, o cliente Jabber não poderá continuar com o login.

Para corrigir isso, certifique-se de que os registros _cisco-uds SRV sejam criados internamente e possam ser resolvidos pelo Expressway-C.

Mais informações sobre os registros SRV DNS podem ser encontradas no [Guia de implantação MRA para X8.11](#).

Esse também é um sintoma comum se você estiver em um domínio duplo. Se você executar em um domínio duplo e descobrir que o cliente Jabber não retornou nenhum UDS (User Data Service), você deve confirmar que os registros SRV _cisco-uds são criados no DNS interno com o domínio externo.

 Observação: após a versão X12.5 do Expressway, não é mais necessário adicionar um registro SRV _cisco-UDS ao DNS interno. Para obter mais informações sobre esse aprimoramento, consulte o [Guia de implantação do Mobile and Remote Access Through Cisco Expressway \(X12.5\)](#).

4. Os logs do Expressway-C mostram este erro: Detalhes de XCP_JABBERD=Não é possível conectar ao host '%IP%', porta 7400:(111) Conexão recusada

Se a placa de rede (NIC) do Expressway-E estiver configurada incorretamente, isso pode fazer com que o servidor XCP (Extensible Communications Platform) não seja atualizado. Se o

Expressway-E atender a esses critérios, você provavelmente encontrará este problema:

1. Usa uma única NIC.
2. A chave de opção de rede avançada está instalada.
3. A opção Usar interfaces de rede duplas está definida como Sim.

Para corrigir esse problema, altere a opção Usar interfaces de rede duplas para Não.

Isso ocorre porque o Expressway-E ouve a sessão XCP na interface de rede errada, o que faz com que a conexão falhe/exceda o tempo limite. O Expressway-E ouve a porta TCP 7400 para a sessão XCP. Você pode verificar isso se usar o comando netstat do VCS como raiz.

5. O nome de host/nome de domínio do servidor Expressway-E não corresponde ao que está configurado no SRV _collab-edge

Se o nome de host/domínio do servidor Expressway-E na configuração de página DNS não corresponder ao que foi recebido na resposta SRV _collab-edge, o cliente Jabber não poderá se comunicar com o Expressway-E. O cliente Jabber usa o elemento xmppEdgeServer/Address na resposta get_edge_config para estabelecer a conexão XMPP com o Expressway-E.

Este é um exemplo de como o xmppEdgeServer/Endereço se parece na resposta get_edge_config do Expressway-E para o cliente Jabber:

```
<xmppEdgeServer>
<server>
<address>examplelab-vcse1.example URL</address>
<tlsPort>5222</tlsPort>
</server>
</xmppEdgeServer>
```

Para evitar isso, certifique-se de que o registro SRV _collab-edge corresponda ao nome de host/nome de domínio do Expressway-E. O bug da Cisco ID [CSCuo83458](#) foi preenchido para isso e o suporte parcial foi adicionado no bug da Cisco ID [CSCuo82526](#).

6. Não é possível fazer logon devido a uma assinatura atual do WebEx Connect

Os logs do Jabber para Windows mostram isso:

```
2014-11-22 19:55:39,122 INFO [0x00002808] [very\WebexCasLookupDirectorImpl.cpp(134)]
[service-discovery] [WebexCasLookupDirectorImpl::makeCasLookupWhenNetworkIs
Available] - makeCasLookupForDomain result is 'Code: IS_WEBEX_CUSTOMER; Server:
http://URL server;
Url: http://example URL server';;.2014-11-22
19:55:39,122 INFO [0x00002808] [overly\WebexCasLookupDirectorImpl.cpp(67)]
[service-discovery] [WebexCasLookupDirectorImpl::determineIsWebexCustomer] -
Discovered Webex Result from server. Returning server result.2014-11-22 19:55:39,122
DEBUG [0x00002808] [ery\WebexCasLookupUrlConfigImpl.cpp(102)]
```

```
[service-discovery] [WebexCasLookupUrlConfigImpl::setLastCasUrl] - setting last_cas_lookup_url : http://example\_URL\_server2014-11-22
19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(286)]
[ConfigStoreManager] [ConfigStoreManager::storeValue] - key : [last_cas_lookup_url]
value : [http://example\_URL\_server/cas/FederatedSSO?org=example\_URL]2014-11-22
19:55:39,123 DEBUG [0x00002808] [common\processing\TaskDispatcher.cpp(29)]
[TaskDispatcher] [Processing::TaskDispatcher::enqueue] - Enqueue ConfigStore::persist
Values - Queue Size: 02014-11-22 19:55:39,123 DEBUG [0x00002808] [pters\config\ConfigStoreManager.cpp(140)]
[ConfigStoreManager] [ConfigStoreManager::getValue] - key : [last_cas_lookup_url]
skipLocal : [0] value: [http://website\_URL/cas/FederatedSSO?org=example\_URL]
success: [true] configStoreName: [LocalFileConfigStore]
```

As tentativas de login são direcionadas ao WebEx Connect.

Para obter uma resolução permanente, você deve entrar em contato com o [WebEx](#) para descomissionar o site.

Solução

A curto prazo, você pode utilizar uma dessas opções para excluí-la da pesquisa.

- Adicione esse parâmetro ao jabber-config.xml. Em seguida, carregue o arquivo jabber-config.xml para o servidor TFTP no CUCM. Ele exige que o cliente faça login internamente primeiro.

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Policies>
    <ServiceDiscoveryExcludedServices>WEBEX<
  /ServiceDiscoveryExcludedServices>
  </Policies>
</config>
```

- Da perspectiva de um aplicativo, execute isto:
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=CUP
EXCLUDED_SERVICES=WEBEX



Observação: a segunda opção não funciona para dispositivos móveis.

- Crie um URL clicável que exclua o serviço WEBEX:
<ciscojabber://provision?ServiceDiscoveryExcludedServices=WEBEX>

Você pode encontrar mais detalhes sobre a descoberta de serviços de UC e como excluir alguns serviços em [Implantação local para o Cisco Jabber 12.8](#).

7. O servidor Expressway-C exibe a mensagem de erro: "Configurado, mas com erros. Servidor de provisionamento: aguardando informações do servidor de passagem."

Se você navegar para Status > Unified Communications e vir a mensagem de erro, "Configurado, mas com erros. Servidor de provisionamento: aguardando informações do servidor de passagem." Para registros do Unified CM e do Serviço IM&P, os servidores DNS internos configurados no Expressway-C têm dois registros DNS A para o Expressway-E. A razão por trás de vários registros DNS A para o Expressway-E pode ser que o usuário afetado mudou de uma única placa de rede com NAT estático habilitado no Expressway-E para uma placa de rede dupla com NAT estático habilitado, ou vice-versa, e esqueceu de excluir o registro DNS A apropriado nos servidores DNS internos. Portanto, ao usar o utilitário de pesquisa DNS no Expressway-C e resolver o FQDN do Expressway-E, você perceberá dois registros DNS A.

Solução

Se a placa de rede do Expressway-E estiver configurada para uma única placa de rede com NAT estático:

1. Exclua o registro DNS A do endereço IP interno do Expressway-E nos servidores DNS configurados no Expressway-C.
2. Limpe o cache DNS no Expressway-C e o PC do usuário via CMD (ipconfig /flushdns).
3. Reinicialize o servidor Expressway-C.

Se a placa de rede do Expressway-E estiver configurada para placa de rede dupla com NAT estático habilitado:

1. Exclua o registro DNS A do endereço IP externo do Expressway-E nos servidores DNS configurados no Expressway-C.
2. Limpe o cache DNS no Expressway-C e no PC do usuário via CMD (ipconfig /flushdns).
3. Reinicialize o servidor Expressway-C.

8. Microsoft DirectAccess Instalado

Se você usar o Microsoft DirectAccess no mesmo PC que o cliente Jabber, quando tentar fazer logon remotamente, isso poderá interromper a MRA. O DirectAccess força as consultas DNS a serem encapsuladas na rede interna como se o PC usasse uma VPN.

 Observação: o Microsoft DirectAccess não é compatível com Jabber sobre MRA. Qualquer solução de problemas é o melhor esforço. A configuração do DirectAccess é de responsabilidade do administrador da rede.

Às vezes, você pode bloquear com êxito todos os registros DNS na Tabela de Políticas de Resolução de Nomes do Microsoft DirectAccess. Esses registros não são processados pelo DirectAccess (o Jabber precisa ser capaz de resolvê-los por meio de DNS público com MRA):

- registro SRV para _cisco-uds
- Registro SRV para _cuplogin
- Registro SRV para _collab-edge
- Um registro para todas as Expressway Es

9. Falhas nas Pesquisas de DNS Reverso do Expressway

A partir da versão X8.8, o Expressway/VCS exige que as entradas de DNS de encaminhamento e reversão sejam criadas para ExpE, ExpC e todos os nós CUCM.

Para obter todos os requisitos, consulte [Pré-requisitos e dependências de software nas Notas de versão x8.8](#) e [Registros DNS para acesso móvel e remoto](#).

Se os registros DNS internos não estiverem presentes, há um possível erro nos logs do Expressway que se referem a reverseDNSLookup:

```
2016-07-30T13:58:11.102-06:00 hostname XCP_JABBERD[20026]: UTCTime="2016-07-30 19:58:11,102" ThreadID="139882696623872"
Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:409" Detail="caught exception: exception in reverseDNSLookup: reverse
DNS lookup failed for address=x.x.x.x"
```

O Expressway-C recebe apenas um FQDN ao consultar o registro PTR do IP do Expressway-E. Se receber um FQDN incorreto do DNS, ele mostrará esta linha nos logs e falhará:

```
2020-04-03T17:48:43.685-04:00 hostname XCP_JABBERD[10043]: UTCTime="2020-04-03 21:48:43,685" ThreadID="140028119959296"
Module="Jabber" Level="WARN " CodeLocation="cvsservice.cpp:601" Detail="Certificate verification failed for host=xx.xx.xx.xx, additional
info: Invalid Hostname"
```

Problemas de registro

Softphone não pode se registrar, método SIP/2.0 405 não permitido

Um log de diagnóstico do Expressway-C mostra uma mensagem Método SIP/2.0 405 não permitido em resposta à solicitação de registro enviada pelo cliente Jabber. Isso provavelmente ocorre devido a um tronco de Session Initiation Protocol (SIP) atual entre o Expressway-C e o CUCM com a porta 5060/5061.

<#root>

SIP/2.0 405 Method Not Allowed

```
Via: SIP/2.0/TCP 10.10.40.108:5060;egress-zone=CollabZone;branch=z9hG4bK81e7f5f1c1
ab5450c0b406c91fcbdf181249.81ba6621f0f43eb4f9c0dc0db83fb291;proxy-call-id=da9e25aa-
80de-4523-b9bc-be31ee1328ce;rport,SIP/2.0/TLS 10.10.200.68:7001;egress-zone=Traversa1
Zone;branch=z9hG4bK55fc42260aa6a2e3741919177aa84141920.a504aa862a5e99ae796914e85d35
27fe;proxy-call-id=6e43b657-d409-489c-9064-3787fc4919b8;received=10.10.200.68;rport=
7001;ingress-zone=Traversa1Zone,SIP/2.0/TLS
192.168.1.162:50784;branch=z9hG4bK3a04bdf3;received=172.18.105.10;rport=50784;
ingress-zone=CollaborationEdgeZone
From: <sip:5151@collabzone>;tag=cb5c78b12b4401ec236e1642-1077593a
To: <sip:5151@collabzone>;tag=981335114
Date: Mon, 19 Jan 2015 21:47:08 GMT
Call-ID: cb5c78b1-2b4401d7-26010f99-0fa7194d@192.168.1.162
Server: Cisco-CUCM10.5
CSeq: 1105 REGISTER
```

Warning: 399 collabzone "SIP trunk disallows REGISTER"

Allow: INVITE, OPTIONS, INFO, BYE, CANCEL, ACK, PRACK, UPDATE, REFER, SUBSCRIBE, NOTIFY
Content-Length: 0

Para corrigir esse problema, altere a porta SIP no Perfil de segurança de tronco SIP que é aplicado ao tronco SIP atual configurado no CUCM e a zona vizinha do Expressway-C para o CUCM para uma porta diferente, como 5065. Isso é explicado com mais detalhes neste [vídeo](#). Aqui está um resumo da configuração:

CUCM

1. Crie um novo perfil de segurança de Tronco SIP com uma porta de escuta diferente da 5060 (5065).
2. Crie um Tronco SIP associado ao Perfil de segurança do Tronco SIP e o destino definido para o endereço IP Expressway-C, porta 5060.

Expressway-C

1. Crie uma zona vizinha para CUCM(s) com uma porta de destino diferente de 5060 (5065) para corresponder à configuração do CUCM.
2. Em Expressway-C Settings > Protocols > SIP, certifique-se de que o Expressway-C ainda ouça o 5060 para SIP.

Softphone não pode registrar, Motivo="Domínio desconhecido"

Um log de diagnóstico do Expressway-C mostra Event="Registration Rejected" Reason="Unknown domain" Service="SIP" Src-ip="XXX.XXX.XXX.XXX" Src-port="51601" Protocol="TCP" AOR="sip:XXX.XXX.XXX.XXX".

Para corrigir esse problema, verifique estes pontos:

- O cliente Jabber usa um perfil de segurança de dispositivo seguro no CUCM quando a intenção é não usar um perfil de segurança de dispositivo não seguro?
- Se os clientes Jabber usam um perfil de segurança de dispositivo seguro, o nome do perfil de segurança está no formato FQDN e esse nome FQDN está configurado no certificado Expressway-C como uma SAN?
- Se os clientes Jabber usarem um perfil de segurança de dispositivo seguro, navegue para System > Enterprise Parameters > Security Parameters > Cluster Security Mode e verifique se o modo de segurança de cluster está definido como 1 para verificar se o cluster CUCM foi protegido. Se o valor for 0, o administrador deverá passar pelo procedimento documentado para proteger o cluster.

Softphone não pode registrar, motivo "contagem regressiva ociosa expirada"

Quando você revisar os logs do Expressway-E durante o período de tempo que o cliente Jabber envia em uma mensagem REGISTER, procure um erro de "contagem regressiva ociosa expirada"

como indicado no trecho de código aqui.

```
<#root>
```

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"  
Module="network.tcp" Level="DEBUG": Src-ip="
```

```
JabberPubIP
```

```
" Src-port="4211"  
Dst-ip="
```

```
VCS-E_IP
```

```
" Dst-port="
```

```
5061
```

```
" Detail="
```

```
TCP Connecting
```

```
"
```

```
2015-02-02T19:46:31+01:00 collabedge tvcs: UTCTime="2015-02-02 18:46:31,144"  
Module="network.tcp" Level="DEBUG": Src-ip="
```

```
JabberPubIP
```

```
" Src-port="4211" Dst-ip=  
"
```

```
VCS-E_IP
```

```
" Dst-port="
```

```
5061
```

```
" Detail="
```

```
TCP Connection Established
```

```
"2015-02-02T19:46:49+01:00  
collabedge tvcs: UTCTime="2015-02-02 18:46:49,606"  
Module="network.tcp" Level="DEBUG": Src-port="4211" Dst-ip=  
"
```

```
VCS-E_IP
```

```
" Dst-port="
```

```
5061
```

```
" Detail="
```

```
TCP Connection Closed
```

```
" Reason="
```

```
Idle  
countdown expired
```

```
"
```

Esse snippet indica que a porta 5061 do firewall está aberta; no entanto, não há nenhum tráfego da camada de aplicação que seja passado em um período de tempo suficiente para que a conexão TCP seja fechada.

Se você encontrar essa situação, há um alto grau de probabilidade de que o firewall na frente do Expressway-E tenha a funcionalidade de Inspeção de SIP/Gateway de Camada de Aplicação (ALG) ativada. Para corrigir esse problema, você deve desabilitar essa funcionalidade. Se você não souber como fazer isso, consulte a documentação do produto do fornecedor do firewall.

Para obter mais informações sobre a inspeção/ALG do SIP, consulte o Apêndice 4 do [Guia de implantação da configuração básica do Cisco Expressway-E e Expressway-C](#).

O MRA falha devido ao proxy do telefone configurado no firmware

Um log de diagnóstico do Expressway-E mostra uma falha de negociação de TLS na porta 5061, no entanto, o handshake SSL teve êxito na porta 8443.

```
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,533" Module="network.tcp" Level="DEBUG": Src-port="24646"
Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connecting"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,534" Module="network.tcp" Level="DEBUG": Src-port="24646"
Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Established"
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="developer.ssl" Level="ERROR"
CodeLocation="ppcmains/ssl/tsssl/tsssl_openssl.cpp(67)" Method="::TTSSLErrorOutput" Thread="0x7fae4ddb1700":
TTSSL_continueHandshake: Failed to establish SSL connection
2015-08-04T10:14:23-05:00 expe tvcs: UTCTime="2015-08-04 15:14:23,535" Module="network.tcp" Level="DEBUG": Src-port="24646"
Dst-ip="10.2.0.2" Dst-port="5061" Detail="TCP Connection Closed" Reason="Got EOF on socket"
2015-08-04T10:14:23-05:00 expe tvcs: Event="Inbound TLS Negotiation Error" Service="SIP" Src-port="24646" Dst-ip="10.2.0.2" Dst-
port="5061" Detail="No SSL error available, probably remote disconnect" Protocol="TLS" Level="1" UTCTime="2015-08-04 15:14:23,535"
```

Logs do Jabber:

```
-- 2015-08-04 10:48:04.775 ERROR [ad95000] - [csf.cert.][checkIdentifiers] Verification of identity: 'URL address' failed.
-- 2015-08-04 10:48:04.777 INFO [ad95000] - [csf.cert.][handlePlatformVerificationResultSynchronously] Verification result : FAILURE
reason : [CN_NO_MATCH UNKNOWN]
-- 2015-08-04 10:48:05.284 WARNING [ad95000] - [csf.ecc.handyiron][ssl_state_callback] SSL alert read:fatal:handshake failure
type=eSIP, isRelevant=true, server=URL server name:5061, connectionState=eFailed, isEncrypted=true, failureReason=eTLSFailure,
SSLErrorCode=336151568
type=eSIP, isRelevant=true, server=192.168.102.253:5060, connectionState=eFailed, isEncrypted=false, failureReason=eFailedToConnect,
serverType=ePrimary, role=eNone
-- 2015-08-04 10:48:05.287 ERROR [ad95000] - [csf.ecc.handyiron][secSSLIsConnected] SSL_do_handshake() returned : SSL_ERROR_SSL.
```

A captura de pacote do Jabber mostra uma negociação SSL com o IP Expressway E; no entanto, o certificado enviado não vem deste servidor:

3813	2015-08-05 12:59:30.811036000	192.168.1.89	97.84.35.116	TLSv1	247 Client Hello
3829	2015-08-05 12:59:30.980461000	97.84.35.116	192.168.1.89	TLSv1	1045 Server Hello, Certificate, Certificate Request, Server Hello Done
3883	2015-08-05 12:59:31.313432000	192.168.1.89	97.84.35.116	TLSv1	252 Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
3887	2015-08-05 12:59:31.341712000	97.84.35.116	192.168.1.89	TLSv1	61 Alert (Level: Fatal, Description: Handshake Failure)

```
Handshake Protocol: Certificate
Handshake Type: Certificate (11)
Length: 539
Certificates Length: 536
Certificates (536 bytes)
Certificate Length: 533
Certificate (id-at-commonName=_internal_PP_ct_phoneproxy_file,id-at-organizationalUnitName=STG,id-at-organizationName=Cisco Inc)
  signedCertificate
  algorithmIdentifier (shawithRSAEncryption)
  Padding: 0
  encrypted: 5d1944c311d1741f9b003995eca3b06a0a3e9f2bd49aa60c...
```

O FW tem o Proxy do telefone configurado.

Solução:

Confirme se o FW executa o Proxy do telefone. Para verificar isso, insira o `show run policy-map` comando e ele mostrará algo semelhante a:

```
class sec_sip
inspect sip phone-proxy ASA-phone-proxy
```

Desative o proxy do telefone para que os serviços de telefone se conectem com êxito.

Problemas relacionados a chamadas

Nenhuma Mídia ao Chamar por MRA

Estas são algumas das configurações ausentes e incorretas que podem causar esse problema em implantações de NIC única e dupla:

- O NAT estático não está configurado no Expressway-E em System > Network Interfaces > IP. O NAT na camada de rede ainda precisa ser feito no firewall, mas essa configuração converte o IP na camada de aplicação.
- As portas TCP/UDP não estão abertas no firewall. Para obter uma lista de portas, consulte o [Guia de Configuração de Uso de Portas IP do Cisco Expressway](#).

Uma única placa de rede com implantações de NAT estático não é recomendada. Aqui estão algumas considerações para evitar problemas de mídia:

- Na zona de passagem UC, o Expressway-C precisa apontar para o endereço IP público configurado no Expressway-E.
- A mídia deve ter um "hairpin" ou refletir no firewall externo. Um exemplo de configuração com um firewall Cisco ASA pode ser encontrado em [Configurar reflexão de NAT no ASA para os dispositivos de telepresença do VCS Expressway](#).

Mais informações sobre isso podem ser encontradas no Apêndice 4 do [Guia de implantação da configuração básica do Cisco Expressway-E e Expressway-C](#).

Sem Toque de Retorno ao Chamar sobre MRA para PSTN

Esse problema é devido a uma limitação no Expressways antes da versão X8.5. O bug da Cisco ID [CSCua72781](#) descreve como o Expressway-C não encaminha a mídia anterior em 183 Session Progress ou 180 Ringing na zona de passagem. Se você executar as versões X8.1.x ou X8.2.x, poderá atualizar para a versão X8.5 ou, como alternativa, executar a solução relacionada aqui.

É possível usar uma solução alternativa no Cisco Unified Border Element (CUBE) se você criar um perfil SIP que transforma o 183 em um 180 e o aplica no correspondente de discagem de entrada. Por exemplo:

```
voice class sip-profiles 11
response 183 sip-header SIP-StatusLine modify "SIP/2.0 183 Session Progress"
"SIP/2.0 180 Ringing"
```

Depois, eles desabilitariam 180 Early Media no perfil SIP do CUCM > CUBE ou no próprio CUBE no modo de configuração sip-ua.

```
disable-early-media 180
```

Problemas de CUCM e IM&P

Erro ASCII que impede a adição de CUCM

Ao adicionar o CUCM ao Expressway-C, você encontra um erro ASCII que impede a adição do CUCM.

Quando o Expressway-C adiciona o CUCM ao seu banco de dados, ele é executado por meio de uma série de consultas AXL relacionadas às funções get e list. Exemplos disso incluem getCallManager, listCallManager, listProcessNode, listProcessNodeService e getCCMVersion. Após a execução do processo getCallManager, ele é sucedido por um conjunto ExecuteSQLQuery para recuperar todas as relações de confiança do CUCM Call Manager ou tomcat-trusts.

Depois que o CUCM recebe a consulta e a executa, ele reporta todos os seus certificados. Se um dos certificados contiver um caractere não-ASCII, o Expressway gerará um erro na interface da Web semelhante a "codec ascii não pode decodificar o byte 0xc3 na posição 42487: ordinal not in range(128)".

Esse problema é rastreado com o bug da Cisco ID [CSCuo5489](#) e é resolvido na versão X8.2.

Falhas de TLS de saída no 5061 do Expressway-C para CUCM em implantações seguras

Esse problema ocorre quando você usa certificados autoassinados no CUCM e no Tomcat.pem/CallManager.pem têm o mesmo assunto. O problema é resolvido com o bug da Cisco ID [CSCun30200](#). A solução alternativa para corrigir o problema é excluir o tomcat.pem e desabilitar a verificação de TLS da configuração do CUCM no Expressway-C.

Servidor IM&P Não Adicionado e Erros Encontrados

Quando você adiciona um Servidor IM&P, o Expressway-C relata "Este servidor não é um Servidor IM e Presence" ou "Não é possível se comunicar com o erro HTTP de consulta .AXL "HTTPError:500", o que faz com que o Servidor IM&P não seja adicionado.

Como parte da adição de um servidor IM&P, o Expressway-C usa uma consulta AXL para procurar os certificados IM&P em um diretório explícito. Devido ao bug da Cisco ID [CSCul05131](#), os certificados não estão nesse armazenamento; portanto, você encontra o erro falso.

Questões diversas

O status do correio de voz no cliente Jabber mostra "Não conectado"



Para que o status do correio de voz do cliente Jabber se conecte com êxito, você deve configurar o endereço IP ou o nome de host do Cisco Unity Connection na lista de permissões HTTP no Expressway-C.

Para concluir isso no Expressway-C, execute o procedimento relevante:

Procedimento para as versões X8.1 e X8.2

1. Clique em Configuration > Unified Communications > Configuration > Configure HTTP server allow list.
2. Clique em New > Enter IP/Hostname > Create entry.
3. Faça logoff do cliente Jabber e depois faça logon novamente.

Procedimento para a versão X8.5

1. Clique em Configuration > Unified Communications > Unity Connection Servers.
2. Clique em New > Enter IP/Hostname, User account credentials > Add Address.
3. Faça logoff do cliente Jabber e depois faça logon novamente.

As fotos de contato não aparecem em clientes Jabber através do Expressways

A solução de Acesso Móvel e Remoto utiliza apenas UDS para resolução de Fotos de Contatos. Isso exige que você tenha um servidor Web disponível para armazenar as fotos. A configuração em si é dupla.

1. O arquivo jabber-config.xml deve ser modificado para direcionar os clientes para o servidor Web para resolução de Foto do contato. A configuração aqui faz isso.

```
<Directory>
<DirectoryServerType>UDS</DirectoryServerType>
<PhotoUriWithToken>http://%IP/Hostname%/photo%uid%.jpg<
/PhotoUriWithToken>
<UdsServer>%IP%</UdsServer>
<MinimumCharacterQuery>3</MinimumCharacterQuery>
</Directory>
```

2.
 1. Clique em Configuration > Unified Communications > Configuration > Configure HTTP server allow list.
 2. Clique em New > Enter IP/Hostname > Create entry.
 3. Faça logoff do cliente Jabber e depois faça logon novamente. O Expressway-C deve ter o servidor Web listado na Lista de Permissões do Servidor HTTP.



Observação: para obter mais informações sobre a resolução de Fotos de Contatos UDS, consulte a [Documentação de Fotos de Contatos Jabber](#).

Os clientes Jabber são solicitados a aceitar o certificado Expressway-E durante o login



Verify Certificate



Certificate not valid

Your computer cannot confirm the identity of this server.
This could be an attempt by an unknown party to connect to your computer and access confidential information.
If you are not sure if you should continue, contact your system administrator. Tell the administrator that Cisco Jabber is prompting you to accept the [redacted] certificate.

Show Certificate

Accept

Decline

Esta mensagem de erro pode estar relacionada ao certificado de Borda do Expressway não assinado por uma CA pública confiável pelo dispositivo cliente ou que o domínio está ausente como uma SAN no certificado do servidor.

Para parar o cliente Jabber do prompt de aceitação do certificado Expressway, você deve atender aos dois critérios listados abaixo:

- O dispositivo/máquina que executa o cliente Jabber deve ter o assinante do certificado Expressway-E listado em seu armazenamento de confiança de certificado.



Observação: isso será facilmente obtido se você usar uma autoridade de certificação pública, pois os dispositivos móveis contêm um grande armazenamento confiável de certificados.

- O domínio de registro do Unified CM usado para o registro de borda de colaboração deve estar presente na SAN do certificado Expressway-E. A ferramenta CSR no servidor Expressway oferece a opção de adicionar o domínio de registro do Unified CM como uma SAN; ela será pré-carregada se o domínio estiver configurado para MRA. Se a autoridade de certificação que assinar o certificado não aceitar um domínio como SAN, você também poderá usar a opção "CollabEdgeDNS", que adiciona o prefixo "collab-edge" ao domínio:

Unified CM registrations domains

tp-cisco.com

Format

CollabEdgeDNS

Alternative name as it will appear

DNS:

DNS:collab-edge.tp-cisco.com

Informações Relacionadas

- [Guia de acesso móvel e remoto no Expressways](#)
- [Guia de implantação de criação e uso de certificados do Cisco Expressway](#)
- [Uso da porta IP do Cisco TelePresence Video Communication Server \(Cisco VCS\) para passagem de firewall](#)
- [Guia de implantação e instalação do Cisco Jabber](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

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.