

# Configurar e solucionar problemas de DNS e requisitos de certificado na Federação Microsoft por meio do Expressway para Cisco Meeting Server

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[DNS](#)

[Certificado](#)

[Troubleshoot](#)

[Sintomas e revisão de registro](#)

[Chamada para o Microsoft Lync/Skype](#)

[Chamada do Microsoft Lync/Skype](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve os requisitos DNS e o certificado do Microsoft Lync/Skype for Business de uma federação entre diferentes domínios pela Internet.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Expressway
- CMS (Cisco Meeting Server)
- Servidor Microsoft Lync ou Skype for Business
- CUCM (Cisco Unified Communications Manager)

## Componentes Utilizados

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

- Cisco Expressway X8.9 ou posterior
- Cisco Meeting Server
- Servidor Microsoft Lync 2010, servidor 2013 Lync ou servidor Skype para Business - no local ou hospedado na nuvem (Office365)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

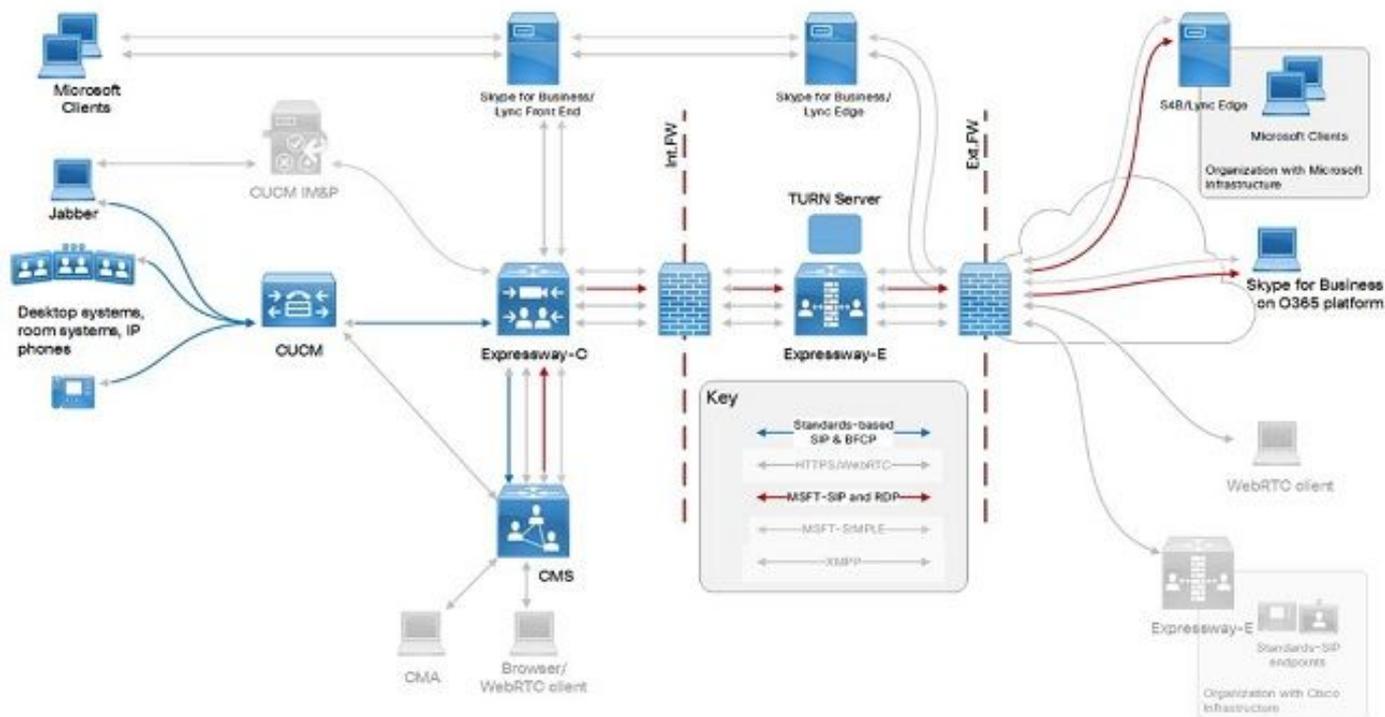
O documento destaca um aspecto específico da integração com clientes Microsoft externos com a Infraestrutura da Cisco usando Expressway e Cisco Meeting Server (CMS). A configuração para essa integração se dá conforme explicado na documentação de **Opções do Cisco Expressway com Cisco Meeting Server e/ou Microsoft Infrastructure disponível para a sua versão** na [lista guias de configuração do Cisco Expressway Series](#) .

O documento atual apenas baseia-se nos requisitos de DNS e o certificado no Microsoft Lync ou Skype for Business para federação externa. As outras configurações são abordadas no guia de configuração mencionado acima.

## Configurar

Um exemplo para o fluxo de chamadas e sua configuração pode ser um endpoint registrado no CUCM que disca para um cliente Skype (no local ou fora do local ou registrado na nuvem usando o Office365) ou vice-versa - usando o CMS para a conversão bentre o protocolo SIP Padrão e Microsoft. Isso é possível por meio da integração b e o roteamento de chamadas usando servidores Expressway, como mostrado na imagem abaixo, que é extraído de **opções de Cisco Expressway com o iguia de configuração Cisco Meeting Server e/ou Microsoft Infrastructure** mencionado no final deste documento.

## Diagrama de Rede



**Note:** Isso é apenas um cenário de fluxo de chamada exemplares. Outros cenários de chamada também são possíveis.

## DNS

O Microsoft Lync/Skype for Business usa o registro SRV `_sipfederationtls._tcp.<domain>` para descobrir os servidores da federação externos para envio de chamadas (bem como informações de presença); ou para a funcionalidade de retorno de chamada com base no domínio especificado no cabeçalho de `From/P-Asserted-Identity` do SIP INVITE de entrada. Neste cenário, os registros DNS devem estar disponíveis no DNS público para ambos os domínios para federação entre si.

A parte do domínio a FQDN (nome de domínio totalmente qualificado) retornada pela pesquisa de registro SRV para o domínio deve ter correspondência exata (nenhum outro domínio ou subdomínio é permitido). A tabela a seguir mostra um exemplo de configuração do DNS para o domínio com o nome `example.com`:

Registro SRV <code>_sipfederationtls._tcp.example.com</code>	<code>expe.example.com</code>
Um registro <code>expe.example.com</code>	O endereço IP de Expressway E

**Caution:** O registro que o SRV resolve deve ser uma correspondência exata no domínio configurado. Subdomínios (por exemplo, `expe.sub.example.com`) ou domínios diferentes (`expe.dummy.com`) não serão confiáveis pelo Microsoft Lync/Skype para Empresas e isso resultará em falhas de chamada mesmo que eles tenham registros A apropriados e resolvam para corrigir IPs.

## Certificado

O Microsoft Lync/Skype for Business configura uma conexão TLS entre os domínios configurados

nos lados do Lync e do Expressway. O Microsoft Lync/Skype for Business tem os seguintes requisitos de certificados de servidor para a federação e os servidores com os quais está se comunicando (Expressway-E neste documento):

- O certificado do servidor apresentado pelo servidor que corresponde ao registro de correspondência deve ter um determinado **FQDN contido em nome alternativo do assunto (ou nome comum, se não usar SAN)**
- O certificado do servidor apresentado pelo servidor precisa ser confiável para servidores Microsoft Lync/Skype for Business (assinados por uma autoridade de certificação pública ou por uma autoridade de certificação particular cujos certificados raiz/intermediário foram importados na **lista de CA confiável dos servidores** Microsoft Lync/Skype for Business). Observe que ao usar o Office365, os certificados CA públicos assinados são necessários.

Por exemplo:

O certificado do servidor do servidor Expressway-E correspondente a **expe.example.com**, como mostrado no exemplo acima, deve ter as seguintes entradas mínimas:

- (Apenas se não houver nenhum **nome alternativos do assunto**) **Nome comum** deve ser **expe.example.com**
- (Se os **Nomes alternativos do assunto estiverem disponíveis**) o **Nome alternativo do assunto** deve conter um **expe.example.com** de entrada
- O emitente na parte superior da árvore de certificado deve para ser uma CA pública (ou a autoridade de certificação precisaria ser adicionada à **Lista de CA confiáveis dos servidores Microsoft Lync/Skype**)

Note:

O domínio (exemplo.com) em si não precisa ser incluído como um **nome alternativo de assunto**.

## Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

A seção contém informações de registro e rastreamentos que obtidas de uma implantação de laboratório de teste com as seguintes especificações:

- O domínio do Skype é skype.lab
- Domínio UC (Expressway-E, Expressway-C e CUCM) é steven.lab
- Domínio CMS para usuários e espaços é acano.steven.lab (cms.steven.lab também está disponível)

Como é recomendado usar um domínio separado para seu Cisco Meeting Server (diferente do seu domínio UC em UCM/Expressway), é provável que você tenha um domínio diferente no servidor Expressway-E e isso poderá resultar em problemas de integração relacionados ao requisitos na federação SIP no servidor Microsoft Lync/Skype for Business.

## Sintomas e revisão de registro

Quando os requisitos em certificados DNS não corresponderem no lado do servidor Microsoft Lync/Skype, observe os sintomas a seguir:

- Quando é feita uma chamada da sua infraestrutura de UC para o Microsoft Lync/Skype, você vê a chamada de saída na zona DNS de sua Expressway-E para o Skype, mas imediatamente lança um erro de tempo limite de servidor (504), visível na página **Status> Search History (Status > Pesquisar histórico) do Expressway-e:**

2017-03-08 15:42:02 SIP (INVITE) sip.stejanss@skype.lab Microsoft AV Server time-out X64

- Quando uma chamada é feita do Microsoft Lync/Skype em direção à infraestrutura de UC, você não verá a chamada que chega ao Expressway-E como mostrado em **Status > Search History (Status > Pesquisar histórico) do Expressway-E.**

Esta subseção explica como verificar esse cenário, usando o registro em mais detalhes e verificar o que exatamente está configurado incorretamente.

## Chamada para o Microsoft Lync/Skype

Nesse fluxo de chamada, você visualiza o registro de diagnóstico da Expressway-E SIP INVITE indo na direção do Skype (se ele pode resolver o registro SRV **\_sipfederationtls.\_tcp SRV para um FQDN e IP**), seguido imediatamente por uma resposta **504 Server time-out sem mais detalhes conforme mostrado no seguinte snippet de registro :**

```
2017-03-02T08:10:46.240+01:00 vcse tvcs: UTCTime="2017-03-02 07:10:46,240" Module="network.sip"
Level="DEBUG": Action="Received" Local-ip="10.48.36.47" Local-port="25002" Src-ip="10.48.36.6"
Src-port="5061" Msg-Hash="13707918855517357847"
SIPMSG:
|SIP/2.0 504 Server time-out
Via: SIP/2.0/TLS 10.48.36.47:5061;egress-
zone=DNSZone1;branch=z9hG4bK42ee6fd77d32cc8925196770b950b33554.731d73c3f4246d6a255e38a9f695bfc0;
proxy-call-id=6b2a018a-2da5-4013-a7e5-4e1455feadf7;rport;received=10.48.36.47;ms-received-
port=25002;ms-received-cid=100
Via: SIP/2.0/TLS 10.48.36.46:5061;egress-
zone=TraversalZoneClient1;branch=z9hG4bK1f8bbe5926dc6abd06ea964d8fde1450156486;proxy-call-
id=e7e33845-c384-4c28-a42d-016863640fbb;received=10.48.36.46;rport=28119;ingress-
zone=TraversalZoneServer1
Via: SIP/2.0/TLS
10.48.54.160:52768;branch=z9hG4bK6594a02846406f4a5459d5f58a8d26b3;received=10.48.54.160;ingress-
zone=NeighborZoneAcano1SIP
Call-ID: f1b3ad5d-183b-4632-b210-c2f9bec71960
CSeq: 2066245576 INVITE
From: "DX70 Steven" <sip:2000@acano.steven.lab>;tag=9fea3e7d70afd884
To: <sip:stejanss@skype.lab>;tag=C65A7B0A8766A5F1D386474833D07882
Server: RTC/6.0
Content-Length: 0
```

A mesma resposta é mostrada (sem mais informações) independentemente se for uma falha nos registros DNS ou no certificado do servidor do Expressway-E.

Assim, para examinar em mais detalhes, você deve analisar o registro do servidor Lync/Skype Edge, onde pode ver os avisos e erros de acordo com as possíveis falhas ocorridas:

- Possível falha: Resultado FQDN do registro SRV não corresponde exatamente ao domínio como no **cabeçalho From/P-Asserted-Identity do INVITE chegando ao Skype**. Neste trecho de log, o cabeçalho From/P-Asserted-Identity do CONVITE SIP contém **acano.steven.lab** como domínio, mas **\_sipfederationtls.\_tcp.acano.steven.lab** está apontando para **vcse.steven.lab** em vez de **vcse.acano.steven.lab** :

```
TL WARN(TF DIAG) [sfvedge\svedge]0584.0A44::03/02/2017-07:10:46.230.0000773E
(SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(830)) [156659184] $$begin_record
Severity: warning Text: The domain of the message resolved by DNS SRV but none of the FQDNs is
in the same domain Result-Code: 0xc3e93d6f SIPPROXY_E_EPROUTING_MSG_ALLOWED_DOMAIN_NO_SRV_MATCH
SIP-Start-Line: INVITE sip:stejanss@skype.lab SIP/2.0 SIP-Call-ID: f1b3ad5d-183b-4632-b210-
c2f9bec71960 SIP-CSeq: 2066245576 INVITE Peer: vcse.steven.lab:25002 Data:
domain="acano.steven.lab";fqdn1="vcse.steven.lab:5061" $$end_record
```

- Possível falha: O certificado do servidor Expressway-E não contém o FQDN resultante do registro SRV `_sipfederationtls._tcp`. O mesmo SIP INVITE é enviado e `_sipfederationtls._tcp.acano.steven.lab` está apontando para `vcse.acano.steven.lab`, mas o FQDN não está contido na lista SAN de certificados do servidor Expressway-E:

```
TL ERROR(TF DIAG) [sfvedge\svedge]0B60.0D6C::03/02/2017-06:30:40.025.00005602
(SIPStack,SIPAdminLog::WriteDiagnosticEvent:SIPAdminLog.cpp(833)) [3634190282] $$begin_record
Severity: error Text: Message cannot be routed because the peer's certificate does not contain a
matching FQDN Result-Code: 0xc3e93d67 SIPPROXY_E_ROUTING_MSG_CERT_MISMATCH SIP-Start-Line:
INVITE sip:stejanss@skype.lab SIP/2.0 SIP-Call-ID: e144704c-1dd0-4ea7-929f-77e7e071c24c SIP-
CSeq: 1567605805 INVITE Peer: vcse.steven.lab:25001 Data: expected-
fqdn="vcse.acano.steven.lab";certName="vcse.steven.lab";info="The peer certificate does not
contain a matching FQDN" $$end_record
```

## Chamada do Microsoft Lync/Skype

Para esse fluxo de chamada, você não vê muito no registro do Expressway-E, pois o servidor Skype Edge servidor não envia INVITE e você precisa contar com o registro no Skype. Use o registro do servidor Lync/Skype (Edge), ou o registro do cliente Lync/Skype propriamente dito para investigar o problema com mais detalhes.

O registro do cliente Skype em um PC com Windows está disponível no seguinte caminho:

*C:\Users\*

Pode ser útil no caso de usuários do Skype Office365 quando nenhum acesso direto aos servidores Skype está disponível. Nesse registro, você pode ver a mensagem SIP INVITE enviada pelo cliente e a resposta apropriada para isso.

Se você não tiver problemas com requisitos de DNS ou certificado no Skype, conforme neste documento, receberá respostas de tempo limite de servidor 504 (incluindo um motivo da falha) dos servidores Skype:

- Possível falha: Resultado FQDN do registro SRV não corresponde exatamente ao domínio que tentou ser chamado. Esse snippet de registro tenta discar para um usuário ou o espaço com domínio `cms.steven.lab` e o `_sipfederationtls._tcp.cms.steven.lab` está apontando para `vcse.sub.cms.steven.lab`:

```
SIP/2.0 504 Server time-out Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C",
srand="8168D157", snum="38", rspauth="65d8d93b66e5b217115e3b1636bf433c9f5df54a",
targetname="SfBFE.skype.lab", realm="SIP Communications Service", version=4 From: "Steven
Janssens"
```

```
INVITE Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00
ms-diagnostics: 1009;
```

**reason**="No match for domain in DNS SRV results";

**domain**="

**cms.steven.lab**";

**fqdn1**="

**vcse.sub.cms.steven.lab:5061**";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0

- Possível falha: O certificado do servidor Expressway-E não contém o FQDN resultante do registro SRV **\_sipfederationtls.\_tcp**. Este trecho de registro mostra uma tentativa de discagem para um usuário ou espaço com domínio **cms.steven.lab** para o qual **\_sipfederationtls.\_tcp.cms.steven.lab** resolve corretamente para **vcse.cms.steven.lab** mas este FQDN não está contido nos Nomes alternativos do assunto no certificado do servidor Expressway-E (com Nome comum como **vcse.steven.lab**):

**SIP/2.0 504 Server time-out** Authentication-Info: TLS-DSK qop="auth", opaque="FA404B9C", srand="1D8F66EF", snum="49", rspauth="67836c7ffc0f6132b2304006969a219d9252aab", targetname="SfBFE.skype.lab", realm="SIP Communications Service", version=4 From: "Steven Janssens"

**INVITE** Via: SIP/2.0/TLS 10.55.186.71:62937;ms-received-port=62937;ms-received-cid=6DA00 ms-diagnostics: 1010;

**reason**="Certificate trust with another server could not be established";ErrorType="The peer certificate does not contain a matching FQDN";

**tls-target**="

**vcse.cms.steven.lab**";

**PeerServer**="

**vcse.steven.lab**";HRESULT="0x80090322 (SEC\_E\_WRONG\_PRINCIPAL)";source="sip.skype.lab" Server: RTC/6.0 Content-Length: 0

## Informações Relacionadas

- [Guias de configuração do Cisco Expressway Series](#)