

# Configurar y solucionar problemas de requisitos de DNS y certificados en federación de Microsoft de Expressway a Cisco Meeting Server

## Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[DNS](#)

[Certificado](#)

[Troubleshoot](#)

[Síntomas y revisión de registro](#)

[Llamada hacia Microsoft Lync/Skype](#)

[Llamada desde Microsoft Lync/Skype](#)

[Información Relacionada](#)

## Introducción

En este documento se describen los requisitos de DNS y certificados de Microsoft Lync/Skype for Business para una federación entre diferentes dominios a través de Internet.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Expressway
- Cisco Meeting Server
- Servidor Microsoft Lync o Skype for Business
- Cisco Unified Communications Manager

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Expressway X8.9 o versiones superiores

- Cisco Meeting Server (CMS) 2.1.2 o versiones superiores
- Servidor Microsoft Lync 2010, Lync 2013 o Skype for Business en las instalaciones o alojado en la nube (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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

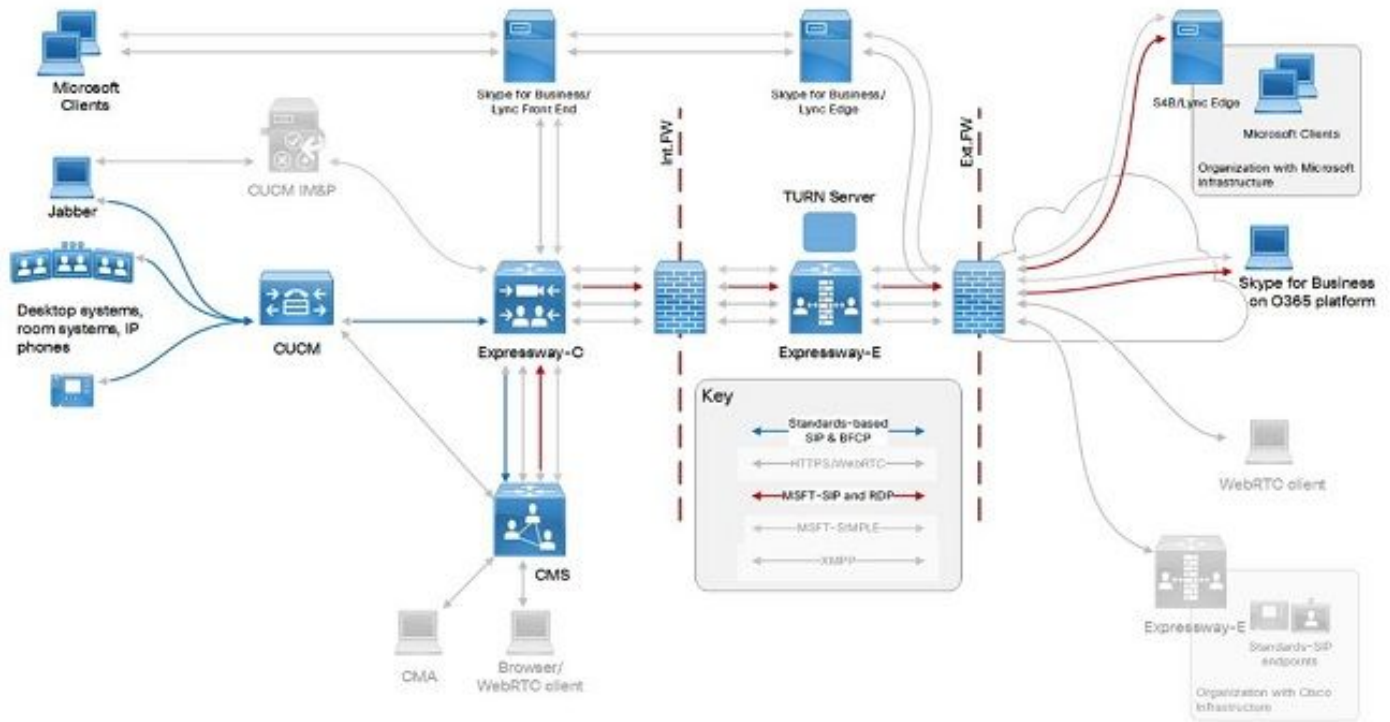
En este documento se resalta un aspecto específico de la integración de clientes externos de Microsoft en su infraestructura de Cisco mediante el uso de Expressway y Cisco Meeting Server (CMS). La configuración para esta integración se explica en la documentación **Opciones de Cisco Expressway con Cisco Meeting Server o infraestructura de Microsoft que está disponible para su versión en la lista de [Guías de configuración de Cisco Expressway Series](#).**

El presente documento se centra particularmente en los requisitos de DNS y certificados de un terminal Microsoft Lync o Skype for Business para una federación externa. Las demás configuraciones se abordan en la guía de configuración antes mencionada.

## Configurar

Un ejemplo del flujo de llamada y su configuración puede ser un terminal registrado CUCM que llama a un cliente Skype (en las instalaciones o fuera de ellas, o registrado en la nube utilizando Office365), o viceversa, mediante el uso de CMS para la conversión entre SIP estándar y protocolo de Microsoft. Esto es posible a través de la integración y el routing de llamadas mediante el uso de servidores de Expressway, como se muestra en la imagen que aparece a continuación, que se tomó de la **guía de configuración de Opciones de Cisco Expressway con Cisco Meeting Server o infraestructura de Microsoft** que se menciona al final de este documento.

## Diagrama de la red



**Nota:** Este es solo un ejemplo de escenario de flujo de llamada. También hay otros escenarios de llamada posibles.

## DNS

Microsoft Lync/Skype for Business utiliza el registro SRV `_sipfederationtls._tcp.<domain>` para **detectar los servidores de federación externa a la que se deben enviar las llamadas (así como información de presencia)** o para la funcionalidad de devolución de llamada según el dominio que se especifica en el encabezado **From/P-Asserted-Identity** del mensaje SIP INVITE entrante. En este caso, los registros de DNS deben estar disponibles en el DNS público para los dos dominios con el fin de realizar la federación mutua.

La parte del dominio del FQDN (nombre de dominio calificado) que arroja la búsqueda de registros SRV para el dominio debe coincidir exactamente (no se permite ningún otro dominio ni subdominio). En la siguiente tabla se muestra un ejemplo de configuración de DNS para el dominio con el nombre **example.com**:

Registro SRV	<code>_sipfederationtls._tcp.example.com</code>	<code>expe.example.com</code>
Un registro	<code>expe.example.com</code>	Dirección IP de ExpresswayE

**Precaución:** El registro A con el que se conecta el SRV debe ser una coincidencia exacta en el dominio configurado. Microsoft Lync/Skype for Business no confiará en los subdominios (por ejemplo `expe.sub.example.com`) o en los diferentes dominios (`expe.dummy.com`) y esto dará lugar a fallas de llamada aunque tengan registros A adecuados y resuelvan corregir las IP.

## Certificado

Microsoft Lync/Skype for Business establece una conexión TLS entre los dominios configurados

en los lados de Lync y Expressway. Microsoft Lync/Skype for Business tiene los siguientes requisitos de certificados de servidor para la federación y los servidores con los que se comunica (Expressway-E en este documento):

- El certificado de servidor presentado por el servidor que coincida con el registro A debe tener el **FQDN específico incluido en su nombre alternativo del sujeto (o nombre común, si no usa SAN)**.
- Los servidores Microsoft Lync/Skype for Business deben confiar en el certificado de servidor presentado por el servidor (ya sea firmado por una CA pública o por una CA privada cuyos certificados raíz/intermedios se han importado en la **lista de CA de confianza de los servidores** Microsoft Lync/Skype for Business). Tenga en cuenta que cuando se utiliza Office365 se requieren certificados firmados por una CA pública.

Por ejemplo:

El certificado de servidor del servidor Expressway-E que coincida con **expe.example.com**, como se muestra en el ejemplo anterior, debe tener los siguientes valores mínimos:

- (Solo si no hay nombres alternativos del sujeto) El nombre común debe ser **expe.example.com**.
- (Si hay nombres alternativos del sujeto disponibles) El nombre alternativo del sujeto debe **contener una entrada expe.example.com**.
- El emisor de la parte superior del árbol de certificados debe ser una CA pública (o la CA se debería agregar en la **lista de CA de confianza de los servidores Microsoft Lync/Skype**).

Nota:

El dominio (example.com) en sí mismo no necesita ser incluido como un **nombre alternativo del sujeto**.

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

En la sección se incluyen información de registro y seguimientos que se han tomado de una implementación de una prueba de laboratorio con las siguientes especificaciones:

- El dominio de Skype es **skype.lab**.
- El dominio de comunicaciones unificadas (Expressway-E, Expressway-C y CUCM) es **steven.lab**.
- El dominio de CMS para los usuarios y los espacios es **acano.steven.lab** (cms.steven.lab también está disponible).

Como se recomienda utilizar un dominio independiente para Cisco Meeting Server (diferente del otro dominio de UC en UCM/Expressway), es probable que disponga de un dominio diferente en el servidor Expressway-E y esto podría ocasionar problemas de integración relacionados con el requisitos de federación SIP en el lado de Microsoft Lync/ Skype del servidor de Business Skype for Business.

## Síntomas y revisión de registro

Cuando los requisitos de certificados de DNS no coincidan en el lado del servidor Microsoft Lync/Skype, observará los siguientes síntomas:

- Cuando se realice una llamada de su infraestructura de UC hacia Microsoft Lync/Skype, verá la llamada saliente en la zona DNS de su Expressway-E a Skype, pero inmediatamente aparecerá un error de tiempo de espera de servidor (504), que se puede ver en la página **Status > Search History (Estado > Historial de búsqueda) de Expressway-E:**

```
2017-03-02T08:10:46.240+01:00 sip INVITE sip:stejanss@skype.lab Microsoft Av Server time-out X64
```

- Cuando se realiza una llamada de Microsoft Lync/Skype hacia su infraestructura de UC, no verá la llamada que llega a Expressway-E, como se muestra en la página **Status > Search History (Estado > Historial de búsqueda) de Expressway-E.**

En esta subsección se explica cómo verificar este escenario mediante el uso de los registros en más detalle y ver qué es exactamente lo que está mal configurado.

## Llamada hacia Microsoft Lync/Skype

En este flujo de llamada, verá en el registro de diagnóstico de Expressway-E el mensaje SIP INVITE que se dirige a Skype (si puede establecer un vínculo del registro SRV **\_sipfederationtls.\_tcp** con un FQDN e IP), a lo que le sigue inmediatamente una respuesta **504 Server time-out** sin más detalles, como se muestra en el siguiente fragmento 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
```

Se muestra la misma respuesta (sin ninguna otra información) independientemente de si se trata de un error en los registros de DNS o en el certificado del servidor de Expressway-E.

Por lo tanto, para revisar esto en mayor profundidad, debe analizar el registro del servidor Lync/Skype Edge, donde puede ver las advertencias y los errores en función de los posibles errores:

- Error posible: El resultado de FQDN del registro SRV no coincide exactamente en el dominio como en el encabezado **From/P-Asserted-Identity** del mensaje INVITE que entra a Skype. En este fragmento de registro, el encabezado **From/P-Asserted-Identity** del SIP INVITE contiene

acano.steven.lab como dominio, pero **\_sipfederationtls.\_tcp.acano.steven.lab** señala a **vcse.steven.lab** en lugar 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
```

- Error posible: El certificado de servidor de Expressway-E no contiene el FQDN obtenido del registro SRV **\_sipfederationtls.\_tcp**. Se envía el mismo mensaje SIP INVITE y **\_sipfederationtls.\_tcp.acano.steven.lab** apunta a **vcse.acano.steven.lab**, pero el FQDN no está incluido en la lista de SAN de certificado del 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
```

## Llamada desde Microsoft Lync/Skype

Para este flujo de llamada no verá muchos detalles en el registro de Expressway-E, ya que el servidor Skype Edge no envía el mensaje INVITE y debe basarse en el registro de Skype. Utilice el registro del servidor Lync/Skype (Edge) o el registro del cliente Lync/Skype para investigar el problema en mayor profundidad.

El registro del cliente Skype en una PC con Windows está disponible en la siguiente ruta de acceso:

```
C:\Users\<username>\AppData\Local\Microsoft\Office\16.0\Lync\Tracing\Lync-UccApi-
x.UccApiLog
```

Puede resultar útil en el caso de los usuarios de Skype Office365 cuando no haya disponible ningún acceso directo a los servidores Skype. En este registro, puede ver el mensaje SIP INVITE enviado por el cliente y la respuesta correspondiente.

Si tiene problemas con requisitos de DNS o certificados en Skype según este documento, recibirá la respuesta **504 Server time-out (incluido un motivo del error)** de los servidores Skype:

- Error posible: El resultado de FQDN del registro SRV no coincide exactamente en el dominio que se intenta llamar. Este fragmento de registro muestra un intento de llamada a un usuario o espacio con dominio **cms.steven.lab** y **\_sipfederationtls.\_tcp.cms.steven.lab** apunta a **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

- Error posible: El certificado de servidor de Expressway-E no contiene el FQDN obtenido del registro SRV **\_sipfederationtls.\_tcp**. Este fragmento de registro muestra el intento de marcar a un usuario o espacio con el dominio **cms.steven.lab** para el que **\_sipfederationtls.\_tcp.cms.steven.lab** resuelve correctamente a **vcse.cms.steven.lab** pero este FQDN no está contenido en los Nombres Alternativos de Asunto del certificado de servidor de Expressway-E (con el nombre común ) **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

## Información Relacionada

- [Guías de configuración de Cisco Expressway Series](#)