

Comprender los requisitos de certificados de acceso remoto y móvil y el historial de ATS

Contenido

[Introducción](#)

[Antecedentes](#)

[En Expressway Versión 14.0.2](#)

[Comportamiento en versiones anteriores a 14.0.8](#)

[Comportamiento en las versiones 14.0.8 y posteriores](#)

[Sección](#)

[Comportamiento en las versiones x15.3](#)

[Qué esperar cuando Callmanager comparte un certificado con varios servicios](#)

[Pasos para reutilizar el certificado](#)

[Historial de versiones del servidor de tráfico Apache](#)

Introducción

Este documento describe los requisitos de carga de certificados en CUCM para acceso móvil y remoto.

Antecedentes

Cisco Expressway utiliza Apache Traffic Server (ATS). El servidor de tráfico es un componente muy importante en las soluciones transversales, que se utiliza principalmente para estas funciones:

- Verificación del certificado: Realiza la verificación de certificados de los nodos de servidor de Cisco Unified Communications Manager (CUCM), IM y presencia, y Unity para los servicios MRA.
- Proxying y caching: Actúa como un servidor proxy de almacenamiento en caché rápido y escalable para el tráfico HTTP/HTTPS.

En Expressway Versión 14.0.2

El servidor de tráfico (ATS) comienza a ver una leve aplicación de la 'verificación de certificados' cuando se comunica con CUCM durante el aprovisionamiento de MRA.

El requisito se documentó en [CSCvz45074](https://cdetsng.cisco.com/summary/#/defect/CSCvz45074), donde los certificados raíz que firmaron los certificados de servidor de núcleo de Expressway deben cargarse en CUCM como Tomcat-Trust y Callmanager Trust: <https://cdetsng.cisco.com/summary/#/defect/CSCvz45074>.

- Servidor de tráfico aplica la verificación de certificados.
- Antes de actualizar a la versión X14.0.2, asegúrese de que se cumpla este requisito de certificado.

Requisito: la cadena de la autoridad certificadora (CA) (raíz + intermediario) que firmó el certificado de Expressway-C debe agregarse a la lista de confianza de Tomcat y CallManager de CUCM, incluso si Unified Communications Manager (UCM) está en modo no seguro.

Motivo: el servicio de servidor de tráfico de Expressway envía su certificado cada vez que un UCM de servidor lo solicita. Estas solicitudes son para servicios que se ejecutan en puertos distintos de 8443 (por ejemplo, puertos 6971, 6972, etc.). Esto aplica la verificación del certificado incluso si UCM está en modo no seguro. Para obtener más información, vea [Guía de implementación de Acceso móvil y remoto a través de Expressway](#).

Comportamiento en versiones anteriores a 14.0.8

El servidor de tráfico de Expressway-C que administra conexiones bidireccionales HTTPS seguras entre Expressway-C y los nodos de Unified Communication no verificó el certificado presentado por el extremo remoto. En la configuración de MRA, existe la opción de tener la verificación del certificado TLS mediante la configuración del modo de verificación de TLS en 'On' cuando se agregan servidores CUCM, IM&P o Unity en Configuration > Unified Communications > Unified CM servers/IM and Presence Service nodes/Unity Connection servers. La opción de configuración se muestra en la siguiente captura de pantalla, que indica que verifica el FQDN o la IP en la SAN, así como la validez del certificado y si está firmado por una CA de confianza.

También hubo un problema conocido en el que no se pueden cargar dos certificados con el mismo nombre CN en el almacén de confianza de Expressway. Esta limitación causó dos problemas:

1. Si elige cargar el certificado del administrador de llamadas en el almacén de confianza de Expressway, la verificación de TLS 'On' fallará al agregar CUCM.

2: Si elige cargar el certificado Tomcat en el almacén de confianza de Expressway, los registros de SIP seguros en 5061 fallarán.

Este comportamiento se documenta en [CSCwa12894](#).

Además, esta verificación de certificado de TLS solo se realiza al detectar los servidores CUCM/IM&P/Unity y no en el momento del aprovisionamiento del cliente MRA.

El inconveniente de esta configuración es que sólo la comprueba para la dirección del editor que agrega. No valida si el certificado de los nodos del suscriptor se ha configurado correctamente, ya que recupera la información del nodo del suscriptor (FQDN o IP) de la base de datos del nodo del editor.

CISCO Cisco Expressway-C

Status > System > Configuration > Applications > Users > Maintenance >

This system has 0 alarms

You are here: Configuration > Unified Communications > Unified CM servers > Edit

Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

Unified CM server lookup

Unified CM publisher address: cucmpubnew.lomcat.com

Username: *comvadmin

Password: ******

TLS verify mode: On

Deployment: lomcat.com

AES GCM support: Off

SIP UPDATE for session refresh: Off

ICE Passthrough support: Off

Save Delete Cancel

Currently found Unified CM nodes				
Name	UCM Version	Zone Protocol	Zone Status	Role
10.106.79.106	15.0.1.12960(234)	TCP	TCP Address resolvable	Subscriber
**10.106.79.102	15.0.1.12960(234)	TCP	TCP Address resolvable	Publisher

Information

If TLS verify mode is enabled, the Unified CM system's FQDN or IP address must be contained within the X.509 certificate presented by that system (in either the Subject Common Name or the Subject Alternative Name attributes of the certificate). The certificate itself must also be valid and signed by a trusted certificate authority.

Default: On

Comportamiento en las versiones 14.0.8 y posteriores

A partir de la versión X14.0.8, el servidor de Expressway realiza la verificación de certificados TLS para cada solicitud HTTPS que se realiza a través del servidor de tráfico. Esto significa que también realiza esto cuando el modo de verificación de TLS se establece en 'Off' durante la detección de los nodos CUCM/IM&P/Unity. Cuando la verificación no tiene éxito, el intercambio de señales TLS no se completa y la solicitud falla, lo que puede llevar a la pérdida de funcionalidad como redundancia, problemas de conmutación por fallas o fallas de inicio de sesión completas, por ejemplo. Además, con el modo de verificación de TLS establecido en 'Activado', no garantiza que todas las conexiones funcionen correctamente como se describe en el ejemplo posterior.

Los certificados exactos que verifica Expressway hacia los nodos CUCM/IM&P/Unity son los que se muestran en la sección de la [guía de MRA](#).

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X15-0/mra/exwy_b_mra-deployment-guide-x150.pdf

Sección

Requisitos de certificado > Requisitos de intercambio de certificados

Debido a estos cambios en la forma en que se produce la comunicación entre Expressway-Core y CUCM, se debe garantizar que:

1. Se recomienda utilizar certificados firmados por CA para Acceso móvil y remoto.
2. Cada clúster de Unified CM debe confiar en el certificado de Expressway-C. Para cada clúster, asegúrese de que:
 - Si el modo mixto está habilitado: el certificado de Expressway-C debe estar instalado en el almacén de confianza de CallManager y Tomcat en Unified CM.
 - Si el modo mixto está deshabilitado: el certificado de CA raíz que firma el certificado de Expressway-C debe estar instalado en el almacén de confianza de CallManager y Tomcat en Unified CM. A continuación, reinicie estos elementos: · Servicio Tomcat · Servicio CallManager · Servicio de proxy HA (si utiliza TLS en Tomcat).

En Expressway - Core, asegúrese de realizar estas acciones:

- Expressway-C debe confiar en los certificados presentados por cada clúster de Unified CM, IM y Presence Service.

El almacén de confianza de Expressway-C debe incluir el certificado de CA raíz que firma los certificados de Unified CM, IM y Presence Service para todos los clústeres de UC.



Nota: Asegúrese de agregar todos los certificados de CA raíz e intermedia o la cadena de CA completa utilizada para firmar el certificado de Expressway-C a la lista de confianza de Tomcat y CallManager de Cisco Unified Communications Manager (UCM), aunque UCM esté funcionando en modo no seguro.

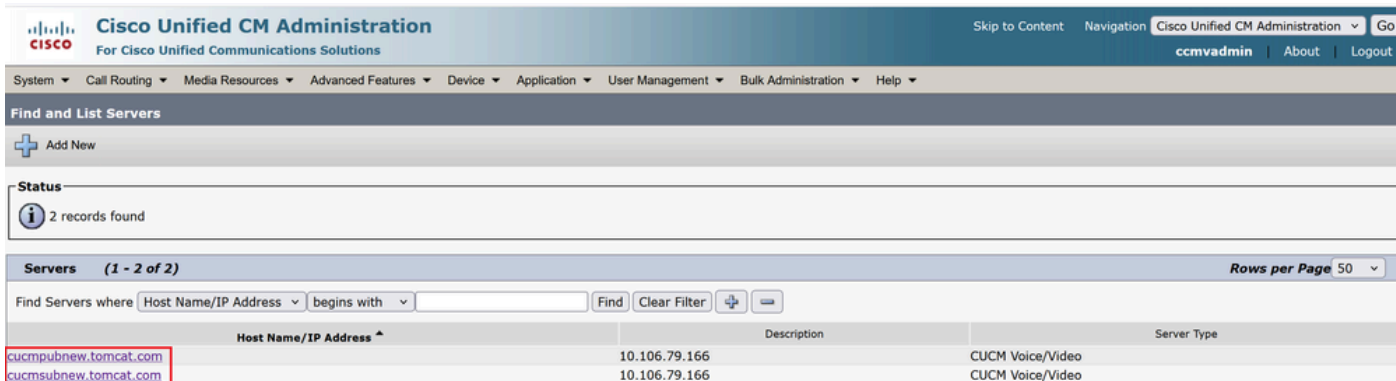
Motivo: el servicio de servidor de tráfico de Expressway envía su certificado cada vez que un servidor (UCM) lo solicita. Estas solicitudes son para servicios que se ejecutan en puertos distintos de 8443 (por ejemplo, puertos 6971, 6972, etc.). Esto aplica la verificación del certificado incluso si UCM está en modo no seguro.

La forma en que se agrega la dirección de CUCM en System > Server desempeña un papel muy importante al agregar CUCM/IMP en el núcleo de Expressway en Configuration > Unified Communications > Unified CM servers/IM and Presence Service nodes.

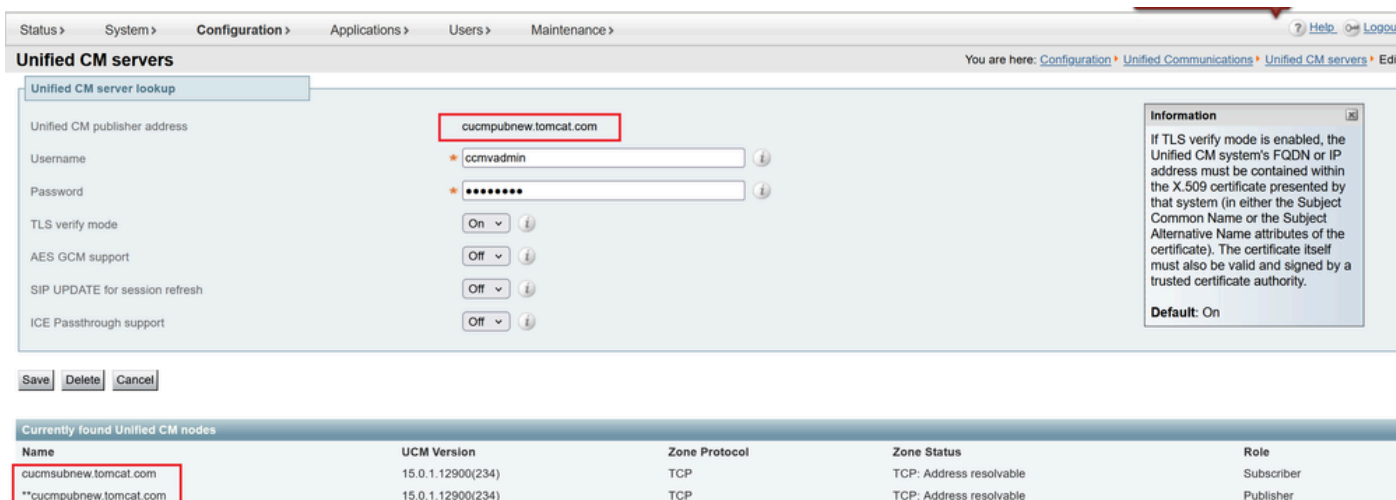
CUCM siempre se debe agregar con FQDN y no con el nombre de host o la dirección IP. Si se ve que CUCM se agrega en System > Server como nombre de host/dirección IP

durante el intercambio de señales de TLS, la verificación de TLS 'On' fallará y el clúster de CUCM no se agregará en Expressway-Core.

Esta figura muestra CUCM agregado como nombre de host:



Esta figura muestra CUCM agregado en Expressway-Core con FQDN con modo de verificación de TLS = ACTIVADO:



También se introdujo un cambio en X14.2 que presentará cifrados durante un intercambio de señales TLS (saludo del cliente) en orden de preferencia diferente. Esto dependía de la trayectoria de actualización y causaba conexiones TLS inesperadas después de una actualización de software. Puede ser que antes de la actualización durante el intercambio de señales de TLS, solicitara el certificado de Cisco Tomcat o Cisco CallManager de CUCM. Sin embargo, después de la actualización, solicitó la variante ECDSA (que es la variante de cifrado más segura que RSA). Los certificados de Cisco Tomcat-ECDSA o Cisco CallManager-ECDSA pueden estar firmados por una CA diferente o, simplemente, pueden ser certificados autofirmados (el valor predeterminado).

Este cambio en el orden de preferencia de cifrado no siempre es relevante para usted, ya que depende de la ruta de actualización, como se muestra en las [notas de la versión de Expressway X14.2.1](#). En pocas palabras, puede ver en Mantenimiento > Seguridad > Cifras para cada una de las listas de cifrado si se antepone ECDHE-RSA-AES256-GCM-SHA384 o no. Si no es así, prefiere el cifrado ECDSA más reciente sobre el cifrado RSA. Si es así, entonces tiene el comportamiento anterior con RSA que tiene la preferencia más alta.

La siguiente captura de pantalla muestra un cifrado ECDSA de cuadro rojo anunciado por el núcleo de Expressway durante el mensaje de negociación TLS en el saludo del cliente, #IF TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 es elegido por el respondedor remoto (CUCM) en el saludo del servidor, entonces la negociación TLS fallará si:

Certificados de CA RAÍZ o certificados ECDSA reales de Responder, es decir, CUCM no está instalado en el almacén de confianza de Expressway en este caso.

```
▼ TLSv1.3 Record Layer: Handshake Protocol: Client Hello
  Content Type: Handshake (22)
  Version: TLS 1.0 (0x0301)
  Length: 512
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 508
    > Version: TLS 1.2 (0x0303)
      Random: b82e6720580ae3f044e8bde95d5a0a2f68b240e720e5a75f4471cdfc25784cf8
      Session ID Length: 32
      Session ID: b18bb9a287a1cc5bcc1087470f608423d4ccd6710f276dff95e5faf613e4716d
      Cipher Suites Length: 66
    ▼ Cipher Suites (33 suites)
      Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
      Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
      Cipher Suite: TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)
      Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
      Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xc03a)
      Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc038)
```

También puede modificar los cifrados de Expressway para que ECDSA no tenga prioridad.

1. Modifique el cifrado SIP agregando una cadena SSL abierta GCM-Sha384.

"ECDHE-RSA-AES256-GCM-SHA384:EECDH:EDH:HIGH:.....:IMD5:IPSK:!eNULL:!aNULL:!aDH"

2. Agregue + para mover el cifrado en la última preferencia o agregue ! para inhabilitar ECDSA permanentemente.

Cifrado: "EECDH:EDH:HIGH:-
AES256+SHA:IMEDIUM:LOW:3DES:IMD5:IPSK:!eNULL:!aNULL:!aDH:+ECDSA"

3. Agregue el certificado de CA raíz e intermedia que firmó el certificado ECDSA en CUCM o agregue el certificado Tomcat-ECDSA en el almacén de confianza de Expressway (en algunos casos).

Sin embargo, debido al cambio en la precedencia de los cifrados, después de la actualización, las implementaciones de MRA pueden romperse, por lo que el TAC tendrá que realizar la solución alternativa mencionada anteriormente para que todo funcione de nuevo.

Con la introducción de TLS 1.3, se hace aún más difícil verificar qué certificados se intercambian en wireshark.

Comportamiento en las versiones x15.3

Sólo para la interfaz SIP, puede elegir tener cifrados RSA o ECDSA.

Con X15.x se ha aplicado TLS 1.3. Como se ve en el campo, el algoritmo RSA se elige principalmente sobre ECDSA. Los clientes que actualicen a x15.2 ahora pueden elegir

entre RSA y el algoritmo ECDSA con este conjunto de comandos:

xConfiguration SIP Advanced TlsSignatureAlgoPrefRsa: Activado/desactivado

TlssignatureAlgoPrefRSA sólo funcionará si la interfaz SIP tiene TLS 1.3

xConfiguration SIP Advanced SipTlsVersiones: "TLSv1.3"

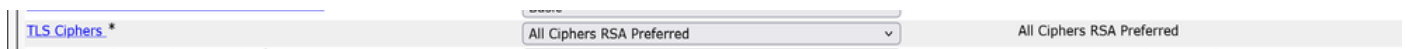


Nota: Solo cumple los requisitos para la interfaz SIP a partir de ahora. Las consideraciones sobre el servidor de tráfico y Tomcat en 8443 no han cambiado, como se ha documentado anteriormente.

Los conjuntos de cifrado enviados durante el "saludo del cliente" por Expressway a CUCM serán como se muestra cuando se elige RSA.

- Algoritmo de firma: rsa_pss_rsae_sha512 (0x0806)
- Algoritmo de firma: rsa_pss_rsae_sha384 (0x0805)
- Algoritmo de firma: rsa_pss_rsae_sha256 (0x0804)
- Algoritmo de firma: ecdsa_secp521r1_sha512 (0x0603)
- Algoritmo de firma: ecdsa_secp384r1_sha384 (0x0503)
- Algoritmo de firma: ecdsa_secp256r1_sha256 (0x0403)

La configuración anterior funcionará en tándem en la configuración que haya elegido en CUCM para los cifrados TLS en Parámetros de empresa > Parámetros de seguridad.



Además, es importante tener en cuenta que durante un intercambio de señales de TLS roto sobre TLS 1.3 entre Expressway-C y CUCM, los errores impresos en los registros de diagnóstico o PCAP no son muy útiles. Vale la pena habilitar estas depuraciones mientras se trabaja con TAC, de modo que el componente imprima errores claros para resolver problemas.

Desarrollador de xConfiguration Logger Nivel developer.trafficserver.http: "DEPURAR"

Desarrollador de xConfiguration Logger Developer developer.trafserver.http_trans Nivel: "DEPURAR"

Desarrollador de xConfiguration Logger Developer developer.trafserver.iocore Nivel: "DEPURAR"

Desarrollador de xConfiguration Logger Nivel developer.trafficserver.ssl: "DEPURAR"

Qué esperar cuando Callmanager comparte un certificado con varios servicios

Las cosas cambian ligeramente con la reutilización del certificado en CUCM.

A partir de CUCM 14.0, puede reutilizar los certificados de Tomcat y Tomcat ECDSA como Call manager y Call manager ECDSA.

El certificado Tomcat se puede reutilizar como certificado de Callmanager.

El certificado Tomcat-ECDSA se puede reutilizar como certificado Callmanager-ECDSA.

Esto hace la vida fácil.

1. Varios servicios de CUCM utilizan ahora un certificado, lo que reduce el coste del certificado.

2. Menos gestión de certificados.

3. Si necesita cargar el certificado Tomcat/Callmanager o Tomcat-ECDSA/Callmanager-ECDSA (por cualquier motivo) en el almacén de confianza de Expressway-Core, será solo un certificado que necesita cargar. No habrá ningún problema de tener el mismo problema con el nombre CN (ya se ha hablado anteriormente en este documento).



Nota: La reutilización del certificado solo se producirá cuando Tomcat y Tomcat-ECDSA sean certificados multiservicio.

Los certificados de servidor ECDSA de Post Reuse, Callmanager y Callmanager no están visibles en el almacén de confianza de CUCM. Puede validar la reutilización de certificados desde CLI ejecutando comandos:

```
show cert own CallManager
```

```
show cert own tomcat
```


Pasos para reutilizar el certificado

Generación de Tomcat CSR pub add.

Certificate Details for cucmpubnew-ms.stark.com, tomcat

 Regenerate  Generate CSR  Download .PEM File  Download .DER File

Status

 Status: Ready

Certificate Settings

Locally Uploaded	06/09/25
File Name	tomcat.pem
Certificate Purpose	tomcat
Certificate Type	certs
Certificate Group	product-cpi
Description(friendly name)	Certificate Signed by WIN-9G89V8O9OR2

Certificate File Data

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      48:00:00:00:04:61:fc:d3:8c:8f:a1:12:92:00:00:00:00:00:04
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC = com, DC = stark, CN = WIN-9G89V8O9OR2
    Validity
      Not Before: Sep  6 05:07:47 2025 GMT
      Not After : Sep  6 05:17:47 2027 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.stark.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
```

Regenerate

Generate CSR

Download .PEM File

Download .DER File

Cargue el certificado de CA que firmará el certificado Tomcat en CUCM como Tomcat-trust.

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* tomcat-trust

Description(friendly name)

Upload File Browse... shashaCA.cer

Upload Close

i *- indicates required item.

Una vez firmado el certificado de Tomcat, cárguelo en el editor. Reinicie los servicios relevantes cuando se le solicite.

Upload Certificate/Certificate chain

Upload Close

Status

i Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* tomcat

Description(friendly name)

Upload File Browse... pubcucmtomcat15.cer

Upload Close

i *- indicates required item.

Una vez firmado el certificado de Tomcat, cárguelo en el editor. Reinicie los servicios relevantes cuando se le solicite.

Éxito: Certificado cargado. Realice una copia de seguridad de recuperación ante desastres para que la copia de seguridad más reciente contenga el certificado cargado.

Reinicie el servicio web de Cisco Tomcat mediante la CLI 'utils service restart Cisco Tomcat' en todos los nodos de clúster (UCM/IMP). Reinicie los servicios web de Cisco UDS Tomcat y Cisco

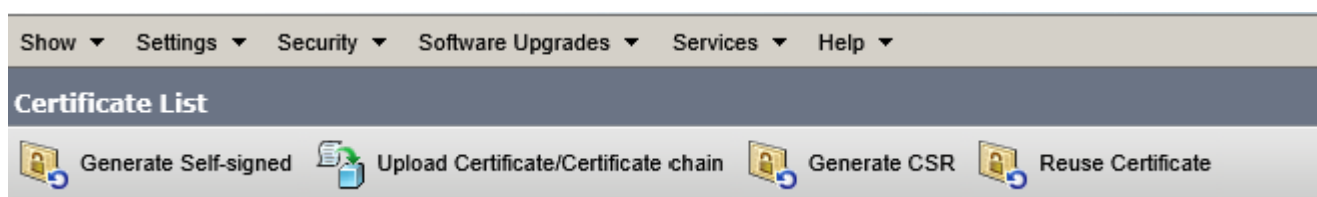
AXL Tomcat mediante la CLI 'utils service restart Cisco UDS Tomcat y utils service restart Cisco AXL Tomcat' en todos los nodos de clúster de UCM. Además, reinicie los servicios Cisco DRF Master y Cisco DRF Local en el nodo del editor. Reinicie solamente el servicio local de Cisco DRF en los nodos del suscriptor.

El certificado Tomcat ahora está firmado por CA.

tomcat	cucmoubnw-ms.stark.com_51dc40f400000000000b	signed IdentityCA- signed	RSA Multi-server(SAN)	RICKY200-TMS-CA	10/23/2027 Certificate Signed by RICKY200-TMS-CA
--------	---	---------------------------------	-----------------------	-----------------	--

Para reutilizar el certificado Tomcat como certificado de Callmanager ahora.

Haga clic en Reutilizar certificado.



Elija Tomcat en el menú desplegable y verifique el certificado de Callmanager.



Haga clic en Finish (Finalizar).

Use Tomcat Certificate For Other Services

Finish Close

Status

- Certificate Successful Provisioned for the nodes cucmpubnew.stark.com,cucmsubnew.stark.com,.
- Restart Cisco HAProxy Service for the generated certificates to become active.
- If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Source

Choose Tomcat Type*

Replace Certificate for the following purpose

CallManager
 CallManager-ECDSA

Finish Close

El certificado Tomcat ahora se reutiliza como certificado de Callmanager. Esto se puede validar desde CLI.

Número de serie (SN) del certificado de Callmanager: 56:ff:6c:71:00:00:00:00:0d

```

admin:show cert own CallManager
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      56:ff:6c:71:00:00:00:00:0d
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
    Validity
      Not Before: Oct 24 08:44:34 2025 GMT
      Not After : Oct 24 08:54:34 2027 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.
tomcat.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
        6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
        44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
        10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
        89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
        23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
        5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit

```

SN de certificado de Tomcat: 56:ff:6c:71:00:00:00:00:0d

```
admin:show cert own tomcat
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      56:ff:6c:71:00:00:00:00:0d
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: DC = com, DC = RICKY200, CN = RICKY200-TMS-CA
    Validity
      Not Before: Oct 24 08:44:34 2025 GMT
      Not After : Oct 24 08:54:34 2027 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-ms.tomcat.com
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public-Key: (2048 bit)
      Modulus:
        00:b4:a6:fa:8f:9a:c3:32:02:74:fa:e9:92:30:de:
        6e:3b:70:cd:d7:4e:64:e4:71:04:fe:17:80:0d:5b:
        44:d1:7f:00:63:69:4a:5c:1a:1b:75:0c:1a:d6:ce:
        10:3f:01:e2:d0:f1:75:33:57:b7:0a:71:e1:60:d1:
        89:3c:e8:a4:8c:3e:30:69:4d:4e:98:da:b8:5d:dd:
        23:8c:4d:69:90:69:9d:43:74:84:20:a8:9f:45:dc:
        5a:aa:7b:c8:d1:d0:6f:05:13:d8:99:58:0e:49:7b:
Press <enter> for 1 line, <space> for one page, or <q> to quit
```

Realice los mismos pasos en el suscriptor.

Vamos a firmar el certificado ECDSA ahora para que pueda ser reutilizado como Callmanager-ECDSA.

El certificado Tomcat-ECDSA actual está autofirmado.

tomcat	10.106.79.162_5aceb67f00000000000f	IdentityCA-signed	RSA Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	cucmpubnew-tl.tomcat.com_4b404cf20zfb4/cabf8aedb/8c/1bd4b	identity-self-signed	EC cucmpubnew.tomcat.com	cucmpubnew-tl.tomcat.com	10/23/2023self-signed certificate generated by system

Firme el CSR multisán para el certificado Tomcat-ECDSA.

- Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

- Generate Certificate Signing Request

Certificate Purpose** tomcat-ECDSA

Distribution* Multi-server(SAN)

Common Name* 10.106.79.162

Include OU in CSR

Subject Alternate Names (SANs)

Auto-populated Domains
cucmpubnew.tomcat.com
cucmsubnew.tomcat.com

Parent Domain tomcat.com

Other Domains
ec.vikdutta.com
vcs8c.s.com

No file selected.
Please import .TXT file only.


Key Type** EC

Key Length* 256

Hash Algorithm* SHA256

Firme el certificado mediante CSR y cárguelo.

Upload Certificate/Certificate chain

 Upload  Close

Status



Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*

tomcat-ECDSA

Description(friendly name)

Upload File

Browse...



cucmpubecdsa162.cer

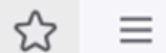
Upload

Close



Upload Certificate/Certificate chain — Mozilla Firefox



  10.106.79.162/cmplatform/certificateUpload.do



Upload Certificate/Certificate chain

 Upload  Close

Status



Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose*

Loading, please wait.

Description(friendly name)

Upload File

Browse...

cucmpubecdsa162.cer

Upload

Close



*- indicates required item.

10.106.79.162

Carga correcta. Reinicie los servicios relevantes cuando se le solicite.

Upload Certificate/Certificate chain

Upload Close

Status

- Certificate upload operation successful for the nodes cucmpubnew.tomcat.com,cucmsubnew.tomcat.com.
- Restart the Cisco Tomcat web service using the CLI "utils service restart Cisco Tomcat" on all cluster nodes (UCM/IMP). Restart Cisco UDS Tomcat and Cisco AXL Tomcat web services using the CLI "utils service restart Cisco UDS Tomcat and utils service restart Cisco AXL Tomcat" on all the UCM cluster nodes. Also, restart the Cisco DRF Master and Cisco DRF Local services on the publisher node. Restart ONLY the Cisco DRF Local service on the subscriber node(s).
- If SAML SSO is enabled, please re-provision the SP metadata on the IDP.

Upload Certificate/Certificate chain

Certificate Purpose* tomcat-ECDSA

Description(friendly name)

Upload File Browse... No file selected.

Upload Close

Tomcat y Tomcat-ECDSA firmados por CA.

tomcat	10.106.79.162_Saceb57f000000000000f	signed	IdentityCA- signed	RSA	Multi-server(SAN)	RICKY200-TMS-CA	10/25/2027Certificate Signed by RICKY200-TMS-CA
tomcat-ECDSA	swmsubnew-CC- ms.tomcat.com_2f0000003880becca8a18e8f2300000000038	signed	IdentityCA- signed	EC	Multi-server(SAN)	bgluclab-WIN-DC-01-CA	10/25/2026Certificate Signed by bgluclab-WIN-DC-01-CA

Ahora reutilice Tomcat-ECDSA como certificado Callmanager-ECDSA.

Use Tomcat Certificate For Other Services

Finish Close

Status

- Tomcat Certificate is Multi-Server Certificate
- Tomcat-ECDSA Certificate is Multi-Server Certificate

Source

Choose Tomcat Type* tomcat-ECDSA

Replace Certificate for the following purpose



CallManager

CallManager-ECDSA






Finish Close

Carga correcta. Reinicie los servicios relevantes cuando se le solicite.

Use Tomcat Certificate For Other Services

 Finish
  Close

Status

-  Certificate Successful Provisioned for the nodes cucmsubnew.tomcat.com,cucmpubnew.tomcat.com,,
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.
-  Restart Cisco TFTP service.
-  Restart Cisco CallManager Service and other relevant services on certificate provisioned nodes.

Source

Choose Tomcat Type*

Replace Certificate for the following purpose

CallManager
 CallManager-ECDSA

Verifique los certificados desde CLI.

Callmanager-ECDSA certificate SN: 2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38

```

admin:show cert own CallManager-ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own CallManager-Ecdsa
Invalid Certificate Name. Certificate Not Found.

admin:show cert own tomcat-ECDSA
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
    Validity
      Not Before: Oct 25 06:46:37 2025 GMT
      Not After : Oct 25 06:46:37 2026 GMT
  
```

SN de certificado de Tomcat-ECDSA: 2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38.

```

admin:show cert own tomcat-ECDSA
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      2f:00:00:00:38:80:be:cc:a8:a1:8e:8f:23:00:00:00:00:00:38
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: DC = com, DC = bgluclab, CN = bgluclab-WIN-DC-01-CA
    Validity
      Not Before: Oct 25 06:46:37 2025 GMT
      Not After : Oct 25 06:46:37 2026 GMT
    Subject: C = IN, ST = karnataka, L = bgl, O = cisco, CN = cucmpubnew-EC-ms.tomcat.com
    Subject Public Key Info:
      Public Key Algorithm: id-ecPublicKey
      Public-Key: (256 bit)

```

Dado que ahora está utilizando un certificado para dos servicios, es decir, un certificado Tomcat para los servicios Tomcat y Callmanager, y Tomcat-ECDSA para los servicios Tomcat-ECDSA y Callmanager-ECDSA, se ha vuelto menos engorroso cargar certificados en el almacén de confianza de Expressway (si es necesario, cargue).

Hacer que TLS verifique 'On' mientras agrega UCM en expressway-core para MRA, ha sido más fácil que nunca. Solo agregando una CA de certificado Tomcat o un certificado de servidor hará el trabajo (porque el certificado se comparte ahora entre Callmanager y el servicio Tomcat).

Unified CM servers

Success: Connection success: The server cucmpubnew.tomcat.com was successfully discovered and queried. Connections established with known cluster nodes. Unchanged: 10.106.79.162, 10.106.79.166

Warning: The CSRF Protection status is automatically enabled after the software upgrade. We recommend keeping CSRF protection Enabled. To change it, please log in to the CLI.

Publisher address	Username	TLS verify mode	Nodes discovered by this lookup	Deployment	AC-S GCM support	SIP UPDATE for session refresh	ICE Passthrough support	Actions
<input type="checkbox"/> cucmice.ice.com	appuser	On	cucmice.ice.com	ice.com	Off	Off	Off	View/Edit
<input type="checkbox"/> cucm11su252.s.com	cucmadmin	Off	cucm11su252.s.com	s.com	Off	Off	Off	View/Edit
<input type="checkbox"/> cucm35.vikidutta.com	appuser	Off	cucm35.vikidutta.com	vikidutta.com	Off	Off	Off	View/Edit
<input type="checkbox"/> cucmpubnew.tomcat.com	ccmadmin	On	10.106.79.166, 10.106.79.162	tomcat.com	Off	Off	Off	View/Edit

Click Refresh servers to refresh the details of the nodes associated

Currently found Unified CM nodes	Name	UCM Version	Zone/Protocol	Zone Status
cucm.eight10.com	**cucm.eight10.com	11.5.1.12900(97)	TCP	TCP: Address resolvable
cucm11su252.s.com	**cucm11su252.s.com	11.5.1.12900(21)	TCP	TCP: Address resolvable
cucm35.vikidutta.com	**cucm35.vikidutta.com	12.5.1.11900(146)	TLS / TCP	TLS: Address resolvable, TCP: Address resolvable
cucmice.ice.com	**cucmice.ice.com	11.5.1.14900(11)	TLS / TCP	TLS: Address resolvable, TCP: Address resolvable
cucmpubnew.tomcat.com	**10.106.79.162	15.0.1.12900(234)	TCP	TCP: Address resolvable
cucmpubnew.tomcat.com	10.106.79.166	15.0.1.12900(234)	TCP	TCP: Address resolvable

Si una actualización a x14.2 o posterior ha causado una interrupción para el Acceso remoto móvil, también puede consultar [este](#) completo documento para resolver el problema.

Historial de versiones del servidor de tráfico Apache

Para verificar la versión en su servidor inicie sesión en root y ejecute `~ # /apache2/bin/httpd -v`.

Expressway x8.11.4

Versión del servidor: Apache/2.4.34 (Unix)

Servidor creado: 12 de noviembre de 2018 19:04:23

Expressway x12.6

Versión del servidor: Apache/2.4.43 (Unix)

Servidor creado: 26 de mayo de 2020 18:27:21

Expressway x14.0.8

Versión del servidor: Apache/2.4.53 (Unix)

Servidor creado: 4 de mayo de 2022 08:52:57

Expressway x15.3

Versión del servidor: Apache/2.4.62 (Unix)

Servidor creado: 16 de julio de 2025 12:10:19

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).