

# Unterstützung der Geschäftskontinuität während der COVID-19-Pandemie - Ressourcen für mobile und Remote-Zugriffslösungen

## Inhalt

[Einführung](#)

[Größe](#)

[Konfigurieren](#)

[Fehlerbehebung](#)

## Einführung

In diesem Dokument wird beschrieben, wie eine Lösung für mobilen und Remote-Zugriff (MRA) mithilfe von Cisco Expressway dimensioniert, konfiguriert und Fehler behoben werden können.

## Größe

Der [MRA-Anwendungshinweis](#) fasst zusammen, wie die vorhandene Kapazität in MRA-Bereitstellungen von Cisco optimiert werden kann, und enthält Hinweise zur Bewertung zusätzlicher Kapazitäten.

Darüber hinaus finden Sie unter [Preferred Architecture](#) Informationen zur Bedarfsbestimmung von Cisco Expressway für [Cisco Collaboration 12.x Enterprise On-Premises-Bereitstellungen, CVD](#), Tabellen 9-8 und 9-9.

## Konfigurieren

- [Mobile und Remote-Zugriff über Cisco Expressway Deployment Guide \(X12.5\)](#) und [Expressway MRA Basic Configuration](#) (video) enthalten schrittweise Anweisungen zur Konfiguration der MRA-Lösung.
- Die Firewall-Anforderungen finden Sie in der [IP-Port-Nutzung von Cisco Expressway](#).
- Einige Bereitstellungen können unterschiedliche interne und externe Domänen haben. Informationen zur [Konfiguration von MRA](#) finden Sie unter [Konfigurieren von mobilem und Remote-Zugriff über Expressway/VCS in einer Multi-Domain-Bereitstellung](#).

## Fehlerbehebung

Wenn die Anmeldung bei Jabber über MRA fehlschlägt, führen Sie die folgenden Schritte aus, um das Problem zu beheben:

**Schritt 1:** Führen Sie den [Collaboration Solutions Analyzer](#) (CSA) mit einer Reihe von Testberechtigungen aus.

CSA ist eine Suite von Tools für Ihre Collaboration-Lösung. CSA unterstützt die verschiedenen Phasen des Lebenszyklus einer Collaboration-Lösung, und speziell für MRA reduziert der Collaboration Edge (CollabEdge) Validator die für die Problembeseitigung erforderliche Zeit erheblich.

CollabEdge Validator ist ein Tool, das MRA-Bereitstellungen durch Simulation eines Client-Anmeldeprozesses validiert. Es werden mehrere Prüfungen durchgeführt:

- Validierung von DNS-Einträgen (Public Domain Name System)
- Externe Verbindungsüberprüfungen
- Expressway-E (Exp-E) SSL-Zertifikate
- Anwendungsflussüberprüfungen für Unified Communications Manager (UCM) und IM & Presence Server (IM&P) Benutzerdatendienste (UDS) Extensible Messaging and Presence Protocol (XMPP) SIP-Registrierung (Session Initiation Protocol)

## Eingabe

Das Tool benötigt mindestens eine Domäne, um die DNS-Konfiguration, die Exp-E-Erkennung, die Konnektivität und die SSL-Exp-E-Zertifikate zu überprüfen. Wenn ein Testbenutzername und ein Testkennwort angegeben werden, kann das Tool die Benutzer- und Gerätekonfiguration von UCM abrufen, eine Authentifizierung gegen IM&P durchführen und ein zugeordnetes Gerät registrieren. Wenn Sie über eine reine Telefonbereitstellung verfügen, aktivieren Sie das Kontrollkästchen, und die IM&P-Prüfungen werden übersprungen.

 Fill in below details

Edge domain	tp.ciscotac.net		*	
Username	hocao			
Password	.....			
<input type="checkbox"/>	Phone only deployment			

Validate MRA deployment

## Beispielausgabe

Die erste angezeigte Sache ist eine Übersicht über den Anmeldeversuch, der einen Überblick darüber gibt, was funktioniert und was fehlschlägt. Ein Beispiel, wenn alles korrekt funktioniert:

## Solution overview

### Edge domain

DNS ✓  
WebEx ✓

### Host analysis

Hostname	TCP connectivity	SSL certificate	MRA login	Softphone
ewaye.ciscotac.net	✓	✓	✓	✓

Wenn etwas nicht funktioniert, ist es sofort in dem Abschnitt sichtbar, dass es fehlschlägt. Weitere Einzelheiten finden Sie in den einzelnen Abschnitten dieses Dokuments.

## Solution overview

### Edge domain

DNS ✓  
WebEx ✓

### Host analysis

Hostname	TCP connectivity	SSL certificate	MRA login	Softphone
ewaye.ciscotac.net	✓	✓	✗	?

### Edge-Domänenvalidierung

In der Edge-Domänenvalidierung werden alle Details zu DNS-Datensätzen angezeigt. Klicken Sie auf das Fragezeichen, um weitere Informationen zur Prüfung anzuzeigen.

## Edge domain

### DNS configuration

✓ **\_collab-edge.\_tls.tp.ciscotac.net**

Host	Priority	Weight	Port	IP address
✓ ewaye.ciscotac.net	0	0	8443	173.38.154.85

✓ **\_cuplogin.\_tcp.tp.ciscotac.net**  
Not resolvable.

✓ **\_cisco-uds.\_tcp.tp.ciscotac.net**  
Not resolvable.

### WebEx configuration

✓ Domain **tp.ciscotac.net** is not enabled for WebEx authentication.

### Externe Konnektivität und SSL-Zertifikatsüberprüfungen für Exp-E

Dieser Abschnitt enthält Details zu den Verbindungs- und Exp-E-Zertifikatsprüfungen für jeden Host, der mit den DNS-Datensätzen erkannt wurde. Das Fragezeichen steht auch hier zur Verfügung, um weitere Informationen darüber zu erhalten, welche Prüfungen durchgeführt werden und warum.

### Edge hosts

#### <·> TCP connectivity ?

Host	8443	5222	5061
ewaye.ciscotac.net	✓	✓	✓

#### SSL certificate ?

Host	Valid	SAN	IP phone trust	Client auth	Server auth
ewaye.ciscotac.net <a href="#">View</a>	✓	✓	✓	✓	✓

Klicken Sie neben dem Hostnamen auf **Anzeigen**, um die Zertifikatsdetailansicht zu öffnen und alle Details der kompletten Kette zur Verfügung zu stellen.

# SSL certificate

ewaye.tp.ciscotac.net

×

## Certificate chain

Full chain available



- ▼ CN: Go Daddy Root Certificate Authority - G2
  - ▼ CN: Go Daddy Secure Certificate Authority - G2
- CN: ewaye.ciscotac.net**

## Summary

**CN:** ewaye.ciscotac.net

**Subject:** OU=Domain Control Validated, CN=ewaye.ciscotac.net

**Issuer:**

C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2

## Detail

**Certificate:**

**Data:**

Version: 3 (0x2)

Serial Number: 13402504543026767831 (0xb9ff42df53ab67d7)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, ST=Arizona, L=Scottsdale, O=GoDaddy.com, Inc., OU=http://certs.godaddy.com/repository/, CN=Go Daddy Secure Certificate Authority - G2

**Validity**

Not Before: Aug 18 13:44:01 2017 GMT

Not After : Mar 21 16:19:00 2019 GMT

Subject: OU=Domain Control Validated, CN=ewaye.ciscotac.net

## Edge-Server

In diesem Abschnitt werden die Edge-Konfigurationsdetails angezeigt. Dies geschieht für jedes vom DNS entdeckte Exp-E.

## Tested edge servers



✓ [ewaye.ciscotac.net](#)

### Single sign-on (SSO)

-  Domain [tp.ciscotac.net](#) is not enabled for SSO.
-  OAuth token with refresh is not enabled.

### Edge configuration

- ✓ Successfully retrieved edge config. ▾
- ✓ Found \_cisco-uds SRV record in edge config: [colcmpub.ciscotac.net:8443](#) [colcmsub.ciscotac.net:8443](#)
- ✓ Found user home cluster: [192.168.0.50:8443](#)
- ✓ Found SIP edge server: [ewaye.ciscotac.net:5061](#)
- ✓ Found XMPP edge server: [ewaye.ciscotac.net:5222](#)
- ✓ Found HTTP edge server: [ewaye.ciscotac.net:8443](#)

Der gesamte Inhalt der Antwort kann ebenfalls erweitert werden.

### Edge configuration

- ✓ Successfully retrieved edge config. ^

#### Details

Edge config XML:

```
<?xml version='1.0' encoding='UTF-8'?>
<getEdgeConfigResponse version="1.0">
  <serviceConfig>
    <service>
      <name>_cisco-uds</name>
      <server>
        <priority>0</priority>
        <weight>0</weight>
        <port>8443</port>
        <address>colcmpub.ciscotac.net</address>
      </server>
    </service>
  </serviceConfig>
</getEdgeConfigResponse>
</serviceConfig>
</getEdgeConfigResponse>
```

## UDS-Server

Für jeden Edge-Server, der ausgewählt werden kann, werden die in `get_edge_config` zurückgegebenen UDS-Server einzeln getestet, bis entweder ein funktionierender Server gefunden wird oder alle Server ausfallen.

## Tested UDS servers



✓ [colcmpub.ciscotac.net](https://colcmpub.ciscotac.net)



### UCM user and device configuration

- ✓ Found Cluster user
- ✓ Found UCM version **11.5.1**
- ✓ Successfully retrieved user configuration. ▾
- ✓ Found users full name: **Hoai Trung Cao**
- ✓ Successfully retrieved jabber-config.xml. ▾
- ✓ No Voice Services Domain in jabber-config.xml or domain matches.

## IM&P-Server

Für jeden Edge-Server, der im Abschnitt Edge Servers ausgewählt werden kann, werden die IM&P-Server (die aus dem Serviceprofil abgerufen werden) einzeln getestet, bis entweder ein funktionierender Server gefunden wird oder alle ausfallen.



## IM&Presence



### IM&P user's configuration

- ✓ Found user's UDS service profile URLs in user config. ▾
- ✓ Successfully retrieved user's UDS service profile. ▾
- ✓ Found IM&P server(s). ▾

[colimp.ciscotac.net](https://colimp.ciscotac.net)

- ✓ Successfully retrieved session key.
- ✓ Successfully retrieved IM&P user configuration. ▾
- ✓ Successfully retrieved one-time password.
- ✓ Successfully logged in to IM&P.

## Softphone-Registrierung

Für jeden Edge-Server, der im Abschnitt "Edge Servers" ausgewählt werden kann, wird die Softphone-Registrierung getestet. Der getestete Softphone-Typ hängt von den Geräten ab, die dem Benutzer zugeordnet sind. Befolgen Sie die folgende Liste mit den Prioritäten: CSF, BOT, TCT, TAB. Für den ausgewählten Edge-Server werden die Exp-C-Server (wie von `get_edge_config` zurückgegeben) und der Unified CM-Server (wie in der CUCM-Gruppe konfiguriert) getestet, bis eine Kombination funktioniert oder alle Server ausfallen.

## Softphone registration



### User's device configuration

- ✓ SIPS port is opened
- ✓ Successfully retrieved device configuration file from UCM. ▾
- ✓ Found user's devices. ▾
- ✓ Found user's device to register: [csfhocao](#)
- ✓ Device Configuration ▾
- ✓ Device's DN: [5010](#)
- ✓ Found Call Manager Group ▾

### Tested Expressway-C paths

- ✓ [192.168.0.20](#)

### Tested CUCM servers

- ✓ [colcmsub.ciscotac.net](#)

- ✓ Successfully registered CSF softphone to CUCM.

**Schritt 2:** Nachdem Sie ermittelt haben, wo der Anmeldevorgang fehlschlägt, können Sie mithilfe der [am häufigsten auftretenden Probleme](#) am [Collaboration Edge](#) feststellen, ob sie mit einem der bekannten Probleme übereinstimmen.

Informationen zur [Installation eines Serverzertifikats auf einem Expressway](#) (Video) finden Sie unter Zertifikate [für Collaboration Edge \(MRA\)](#) oder [Installieren eines Serverzertifikats](#) über CSA.

Wenn Sie einen einzigen Netzwerkschnittstellen-Controller (NIC) mit statischer Network Address Translation (NAT) auf dem Exp-E verwenden und eine Adaptive Security Appliance (ASA) verwenden, lesen Sie [Configure NAT Reflection On the ASA For the VCS Expressway TelePresence Devices](#), um sicherzustellen, dass die NAT-Reflektion korrekt konfiguriert ist.

**Schritt 3:** Wenn Sie Ihr Problem nicht beheben konnten, öffnen Sie ein Ticket im Technical Assistance Center (TAC) mit Expressway-Protokollen und einem Problembericht.

- [Herunterladen von Expressway Diagnostic Logs und Packet Captures](#) (Video)
- [Jabber Desktop-Problembericht](#) (Video)