

Supporting Business Continuity During the COVID-19 Pandemic - Mobile and Remote Access Solution Resources

Contents

[Introduction](#)

[Size](#)

[Configure](#)

[Troubleshoot](#)

Introduction

This document describes how to size, configure, and troubleshoot a Mobile and Remote Access (MRA) solution through Cisco Expressway.

Size

The [MRA Scale Application Note](#) summarizes how to optimize existing capacity in Cisco MRA deployments and includes guidance on how to assess additional capacity.

Additionally, Cisco Expressway sizing information is available in [Preferred Architecture for Cisco Collaboration 12.x Enterprise On-Premises Deployments, CVD](#), Tables 9-8 and 9-9.

Configure

- [Mobile and Remote Access Through Cisco Expressway Deployment Guide \(X12.5\)](#) and [Expressway MRA Basic Configuration](#) (video) provide step-by-step instructions on how the MRA solution is configured.
- Firewall requirements can be found in [Cisco Expressway IP Port Usage](#).
- Some deployments might have different internal and external domains. See [Configure Mobile and Remote Access through Expressway/VCS in a Multi-Domain Deployment](#) for information on how to configure MRA.

Troubleshoot

If Jabber log in over MRA fails, complete these steps in order to troubleshoot the issue:

Step 1. Run [Collaboration Solutions Analyzer](#) (CSA) with a set of test credentials.

CSA is a suite of tools for your collaboration solution. CSA helps during the different phases of a collaboration solution lifecycle, and specifically for MRA, the Collaboration Edge (CollabEdge) validator drastically reduces the time needed to troubleshoot the solution.

CollabEdge validator is a tool that validates MRA deployments by simulating a client log in process. There are several checks done:

- Public Domain Name System (DNS) entry validation
- External connectivity checks
- Expressway-E (Exp-E) SSL certificates
- Unified Communications Manager (UCM) and IM & Presence server (IM&P) related application flow checks User Data Services (UDS) Extensible messaging and presence protocol (XMPP) Session Initiation Protocol (SIP) registration

Input

At a minimum, the tool requires a domain to check the DNS configuration, Exp-E discovery, connectivity, and Exp-E SSL certificates. If a test username and password is provided, the tool will be able to retrieve the user and device configuration from UCM, attempt to authenticate against IM&P, and register an associated device. If you have a phone only deployment, check the checkbox and the IM&P checks will be skipped.

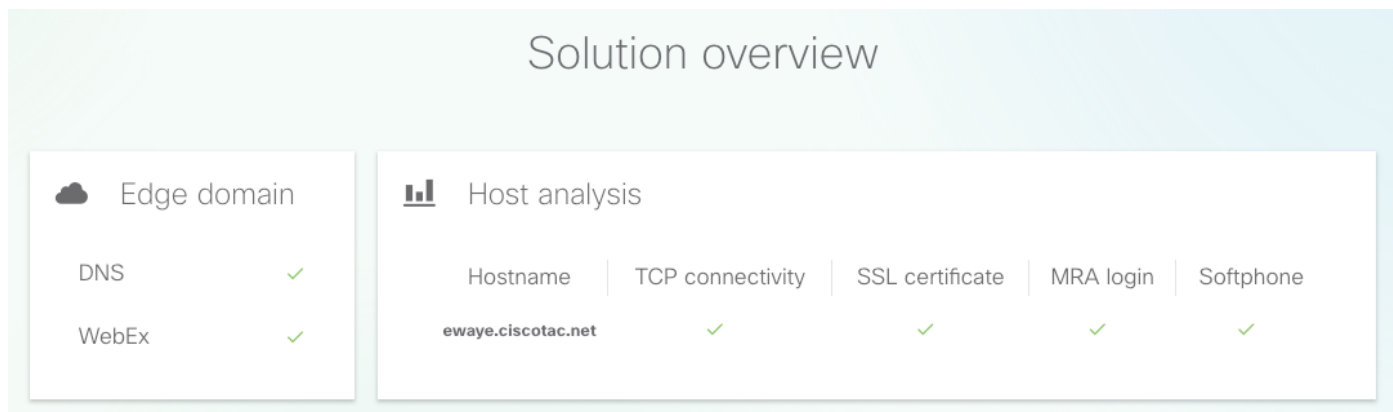
 Fill in below details

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

Validate MRA deployment

Sample Output

The first thing that is displayed is an overview of the log in attempt which gives an overview of what works and what fails. An example when everything works correctly:



When something does not work, it is immediately visible in the section it fails. More details can be found in the specific sections in this document.

Solution overview

Edge domain

DNS ✓

WebEx ✓

Host analysis

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

Edge Domain Validation

In the Edge domain validation all details are displayed with regards to DNS records. Click the question mark in order to display more details about the check.

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.

External Connectivity and Exp-E SSL Certificate Checks

This section shows details about the connectivity and Exp-E certificate checks for each host discovered with the DNS records. The question mark is also available here to obtain more details on what checks are done and why.

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	View	✓	✓	✓	✓

Click **View** next to host name in order to open the certificate detail view and have all details of the complete chain available.

SSL certificate

ewaye.tp.ciscotac.net

×Certificate chainFull 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 Servers



This section shows the Edge configuration details. This is done for every Exp-E discovered by DNS.

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](#)

The full content of the response can be expanded as well.

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>
</xml>
```

UDS Servers

For each Edge server which can be selected, the UDS servers which were returned in the `get_edge_config` are tested one by one until either a working one is found or all of them fail.

Tested UDS servers



✓ 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 Servers

For each Edge server which can be selected in the Edge Servers section, the IM&P servers (fetched from the service profile) are tested one by one until either a working one is found or all fail.



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

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

Softphone Registration

For each Edge server which can be selected in the Edge Servers section, softphone registration is tested. The type of softphone tested depends on the devices associated to the user, and follow this prioritized list: CSF, BOT, TCT, TAB. For the selected Edge server, the Exp-C servers (as returned by `get_edge_config`) and Unified CM server (as configured in the CUCM Group) are tested until a combination works or all of them fail.

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.

Step 2. After you find out where the log in process fails, use [Collaboration Edge Most Common Issues](#) in order to see if it matches one of the known issues.

Refer to [Configure and Troubleshoot Collaboration Edge \(MRA\) Certificates](#) or [Installing a Server Certificate to an Expressway](#) (video) if you find a certificate issue through CSA.

If you use a single Network Interface Controller (NIC) with static Network Address Translation (NAT) on the Exp-E and you use an Adaptive Security Appliance (ASA), see [Configure NAT Reflection On The ASA For The VCS Expressway TelePresence Devices](#) in order to make sure NAT reflection is correctly configured.

Step 3. If you were unable to resolve your issue, open a Technical Assistance Center (TAC) case with Expressway logs and a problem report.

- [Downloading Expressway Diagnostic Logs and Packet Captures](#) (video)
- [Obtaining Jabber Desktop Problem Report](#) (video)