



# Cisco Mobile and Remote Access Best Practices for Optimizing Scale

## Application Note

March 2020

### **Americas Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 527-0883





THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.

---

## Table of Contents

Purpose of this Document .....	5
MRA Overview .....	5
MRA Profile Assessment - Assessing Growth Need .....	5
Optimising Existing Deployments for Increased MRA Use .....	6
Optimising Login - LDAP, UDS and Authentication .....	6
Optimising Login - MRA IM&P Inter Cluster Synch Agent (ICSA) Dependency .....	7
Optimising Resource Consumption on Unified CM and Expressway .....	7
Optimising Resource Consumption During IM&P Processing .....	8
Optimising Traffic .....	8
Increasing Server Resources .....	9
MRA Deployment Best Practice - Software Solution Line-up .....	10
MRA Serviceability .....	11
Counters .....	11
Metrics .....	12
Logs .....	13
Appendix 1 Example Script to List MRA-Registered Devices .....	15
Appendix 2 Find List of Registered Devices - SOAP UI Tool and SXML API .....	17

## Purpose of this Document

COVID-19 is causing an unprecedented challenge for customers to support increasing number of employees working from home (WFH). While Cisco Unified Communications customers with Cisco Jabber can fully leverage standard VPN options to the home, Cisco also supports VPN-less access via Mobile and Remote Access (MRA). Existing customer solutions are typically architected and built to host a much lower percentage of WFH employees than expected.

The purpose of this app note is to provide a summary of best practices to optimize your current deployment, pointers to recommendations for growth/expansion, and links to customer support documents. It gives an overview of the MRA solution and the tools that you can use to assess your existing deployment and its growth needs. It also lists some short-term measures to optimize your existing deployment for increased MRA usage, along with software version recommendations and pointers to aid monitoring and troubleshooting.

## MRA Overview

Cisco Unified Communications Mobile and Remote Access (MRA) is part of the Cisco Collaboration Edge Architecture. It allows endpoints such as Cisco Jabber to have their registration, call control, provisioning, messaging, and presence services provided by Cisco Unified Communications applications such as Unified Communications Manager (Unified CM) or Unified Presence Server (IM&P), when the endpoint is outside the enterprise network. As an example, the Cisco Expressway Series (Expressway) provides secure firewall traversal and line-side support for Unified CM registrations.

More details about MRA are in the *Mobile and Remote Access Through Cisco Expressway Deployment Guide* [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/exwy\\_b\\_mra-expressway-deployment-guide.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_mra-expressway-deployment-guide.pdf)

## MRA Profile Assessment – Assessing Growth Need

Depending on how your deployment is architected you may have to add capacity. The following data will help you to identify your current capacity and how to extrapolate for new pending capacity.

- Expressway capacity requirements can be obtained using the Collab Sizing Tool <https://cucst.cloudapps.cisco.com/>
- Or a simpler alternative to get Expressway capacity information is to use the capacity sizing tables (Table 2 and 3) in the *Cisco Expressway Cluster Creation and Maintenance Guide* [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/Cisco-Expressway-Cluster-Creation-and-Maintenance-Deployment-Guide-X12-5.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/Cisco-Expressway-Cluster-Creation-and-Maintenance-Deployment-Guide-X12-5.pdf)
- Capacity information for Unified Communication Applications can be obtained from <https://cucst.cloudapps.cisco.com/>

**CAUTION:** Cisco tries continuously to improve the accuracy of the sizing tool. However, **the results should be used only for high level planning.**

---

## Optimising Existing Deployments for Increased MRA Use

This section provides some short-term measures that you can explore to leverage your current deployment for increased scale, while you evaluate your solution architecture and plan for capacity augmentation. Ensure that these recommendations are supported on the Unified CM, IM&P, and Expressway versions that you deploy (or plan to deploy). Recommendations about preferred Unified CM, IM&P, Expressway and Jabber software versions for MRA are given later in this document.

### Optimising Login – LDAP, UDS and Authentication

Jabber login for MRA requires additional processing on Unified CM and Expressway. This can lead to spikes in resource consumption during bulk login scenarios. The following recommendations aim to reduce resource consumption during login.

- Enable single sign on (SSO) with IdP using OAuth refresh (self-describing tokens) in place of LDAP authentication. This avoids the need for Expressway to contact Unified CM for LDAP queries and token validation during login. Details of SSO configuration are available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/SAML\\_SSO\\_deployment\\_guide/12\\_5\\_1/cucm\\_b\\_saml-ss0-deployment-guide-12\\_5/cucm\\_b\\_saml-ss0-deployment-guide-12\\_5\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/12_5_1/cucm_b_saml-ss0-deployment-guide-12_5/cucm_b_saml-ss0-deployment-guide-12_5_chapter_01.html).

Details about integrating Unified CM and ADFS for single sign on are available at <https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html>

The procedure to use self-contained tokens on Unified CM and Expressway is available at [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/jabber/11\\_9/Unified-CM-OAuth-Whitepaper-v17-FINAL.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/jabber/11_9/Unified-CM-OAuth-Whitepaper-v17-FINAL.pdf)

- If you are using SSO, it is possible (but not recommended) to increase the validity of access tokens to reduce the number of token refresh requests sent to Unified CM. The default is 60 minutes, but it can be increased to a value up to 1440 minutes. Additionally, the refresh token validity can also be increased beyond the default value of 60 days, up to 1 year. End users would have to re-login with credentials less frequently, with this setting.

**CAUTION:** There is a trade off between reduced security and increased token validity values. We do not recommend increasing these values, but in extraordinary cases some deployments may decide it is worth the risk for the performance gain. Please be certain that you understand the security implications before you do so.

More information on adjusting these parameters is available at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/12\\_0\\_1/systemConfig/cucm\\_b\\_system-configuration-guide-1201/cucm\\_b\\_system-configuration-guide-1201\\_chapter\\_0111000.html#task\\_2B0BB37E9A3CE20B5BF7DF161132BB12](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/systemConfig/cucm_b_system-configuration-guide-1201/cucm_b_system-configuration-guide-1201_chapter_0111000.html#task_2B0BB37E9A3CE20B5BF7DF161132BB12)

- Use the bulk query API for searching contacts from Jabber client. This requires an upgrade to Unified CM version 11.5(SU7) or 12.5(SU2) and Jabber version 12.8.0 or higher.
- If users need to sign in at a specific time of the day, explore the possibility of requesting them to sign in in shifts with a 15-minute offset.
- Ensure that Unified CM upgrades are performed during lean times so that bulk Jabber logins/failovers do not occur. You should expect longer re-login times when there are network outages.

## Optimising Existing Deployments for Increased MRA Use

- We recommend that you populate the URI attribute in LDAP. This avoids email based look-ups by Jabber clients, which are performed individually (not in batches).
- Avoid configuring UDS Proxy on Unified CM if the number of users is less than 160K per cluster. In such cases we recommend using LDAP sync instead, or preferably SSO. UDS Proxy delegates queries to LDAP so that large number of users can be handled without overloading Unified CM, but this can cause higher delays and request queueing.  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab12/collab12.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab12/collab12.html)
- You can push a new *jabber\_config* file to clients to reduce the number of call history records on the client. If possible keep this number to a value less than 100. With bulk query, queries are performed in batches of 100. If bulk query is not in use, an individual query is sent for each record. Note that pushing the config file causes a one-time pop-up to display on the client.

## Optimising Login – MRA IM&P Inter Cluster Synch Agent (ICSA) Dependency

- If IM&P services are required by a Jabber client, failure to login into IM&P services over MRA may cause complete MRA Jabber login failure.
- When connecting over MRA a Jabber device is no longer directly connected to its home IM&P node. Instead, connectivity is established via a mesh of IM&P connections via the Expressway-E and Expressway-C clusters.
- As part of the IM&P sign in process, some stanzas (IM&P protocol packets – session bind) may be routed via other IM&P clusters. These intermediary IM&P clusters therefore need a fully synced user database to ensure that they can forward the IM&P packets to the correct home node for a given user.
- This user database is synchronized between IM&P clusters using the Inter Cluster Synch Agent (ICSA) service. Ensure that this service is running and functioning correctly on all IM&P clusters. The *MRA Serviceability* section later in this document lists the relevant ICSA logs.

## Optimising Resource Consumption on Unified CM and Expressway

MRA call flows require more resources on Unified CM than on-prem calls. These recommendations can reduce CPU usage on Unified CM so that more MRA calls can be accommodated:

- Turn on SIP OAuth if you are using software version 12.5 or later on Unified CM and Expressway. This can reduce the amount of CPU consumed during call processing on Unified CM. SIP OAuth solution design information is available here:  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/12\\_5\\_1/featureConfig/cucm\\_b\\_feature-configuration-guide-1251/cucm\\_b\\_feature-configuration-guide-1251\\_chapter\\_0110100.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/featureConfig/cucm_b_feature-configuration-guide-1251/cucm_b_feature-configuration-guide-1251_chapter_0110100.html)
- Turn off EM, EMCC, IPMA, and Web Dialer applications on Unified CM if desk phones in the office are not being used during this period. Information is available in the Services Setup section here:  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/11\\_5\\_1/Admin/CUCM\\_BK\\_CE\\_F360A6\\_00\\_cisco-unified-serviceability-admin-guide\\_1151/CUCM\\_BK\\_CEF360A6\\_00\\_cisco-unified-serviceability-admin-guide\\_1151\\_chapter\\_0101.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/11_5_1/Admin/CUCM_BK_CE_F360A6_00_cisco-unified-serviceability-admin-guide_1151/CUCM_BK_CEF360A6_00_cisco-unified-serviceability-admin-guide_1151_chapter_0101.html)
- Check for AXL traffic and turn off any integration that does bulk provisioning using AXL.

- 
- You can turn off any desk phones that will not be used during this time and configure Call Forward Unregistered (CFUR) to mobile phones for these devices. CFUR configuration information is available here:  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/12\\_0\\_1/featureConfig/cucm\\_b\\_cucm-feature-configuration-guide\\_1201/cucm\\_b\\_cucm-feature-configuration-guide\\_1201\\_chapter\\_011010.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_0_1/featureConfig/cucm_b_cucm-feature-configuration-guide_1201/cucm_b_cucm-feature-configuration-guide_1201_chapter_011010.html)
- NOTE:** You can get a list of registered phones from Unified CM before turning them off, so that you can verify their status later when the phones are turned on. (To get the list of registered devices in the Unified CM Publisher using the Serviceability API, follow the steps in Appendix 2 Find List of Registered Devices - SOAP UI Tool and SXML API.)
- You can turn off UDS and CCM services on the Unified CM Publisher node if your Expressway version is X12.5.7 or higher.

## Optimising Resource Consumption During IM&P Processing

Presence computation takes up a significant amount of CPU on IM&P servers. You can turn off some forms of presence computation, depending on how reliant your workflows are on Presence.

- Turn off temporary Presence completely.  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/im\\_presence/configAdminGuide/12\\_5\\_1/cup0\\_b\\_config-and-admin-guide-1251/cup0\\_b\\_config-and-admin-guide-1251\\_chapter\\_01110.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/12_5_1/cup0_b_config-and-admin-guide-1251/cup0_b_config-and-admin-guide-1251_chapter_01110.html)
- Disable 'Click2X' functionality on Jabber clients to disable refreshing temporary Presence on distribution lists for received outlook emails. This must be done by the end user for each client.  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/11\\_0/CJAB\\_BK\\_D657A25F\\_00\\_deployment-installation-guide-jabber-110/CJAB\\_BK\\_D657A25F\\_00\\_deployment-installation-guide-jabber-110\\_chapter\\_01100.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/11_0/CJAB_BK_D657A25F_00_deployment-installation-guide-jabber-110/CJAB_BK_D657A25F_00_deployment-installation-guide-jabber-110_chapter_01100.html)
- If you use enterprise AD groups for IM&P groups, you can apply a lower group size limit for sending Presence updates. This improves CPU usage on IM&P nodes, but will cause Presence updates to be turned off on groups larger than the configured limit.  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/im\\_presence/configAdminGuide/12\\_5\\_1/cup0\\_b\\_config-and-admin-guide-1251/cup0\\_b\\_config-and-admin-guide-1251\\_chapter\\_01110.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/12_5_1/cup0_b_config-and-admin-guide-1251/cup0_b_config-and-admin-guide-1251_chapter_01110.html)

## Optimising Traffic

- Turn off video where possible, as this is a great way to reduce load on the Expressway nodes. You can configure per-call bandwidth limits on Unified CM for groups of users for whom video has to be turned off. The configured bandwidth limit should allow only audio calls ( $\leq 128$  kbps).

The following link specifies how to configure the Region setting for device groups and how to configure **Maximum Session Bit Rate for Video Calls** to *None* to disable video for calls between and within the Region groups.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/9\\_1\\_1/ccmcfq/CUCM\\_BK\\_A34970C5\\_00\\_admin-guide-91/CUCM\\_BK\\_A34970C5\\_00\\_admin-guide-91\\_chapter\\_0111.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_1_1/ccmcfq/CUCM_BK_A34970C5_00_admin-guide-91/CUCM_BK_A34970C5_00_admin-guide-91_chapter_0111.html)

- You can configure PSTN fall-back for specific groups of phones. Call Forward (CFNA/CFA) can be configured on Unified CM for desk phones so that calls are routed to PSTN numbers (mobile phones or land lines).

## Optimising Existing Deployments for Increased MRA Use

- Enable ICE Passthrough on Expressway to optimize MRA-MRA calls. This ensures that:
  - Media flow between two MRA endpoints takes an optimized path where possible.
  - Limits the processing done on Expressway, and the bandwidth consumed for Internet connectivity from your data center.

ICE Passthrough is available from versions 12.5 and above for Unified CM and Expressway. Instructions to to configure it are in the following link.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-5/exwy\\_b\\_mra-expressway-deployment-guide/exwy\\_b\\_mra-expressway-deployment-guide\\_chapter\\_01100.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-5/exwy_b_mra-expressway-deployment-guide/exwy_b_mra-expressway-deployment-guide_chapter_01100.html)

- Configure use of low-bandwidth codecs - such as Opus, iLBC or G.729 - for selected MRA devices. Identify the MRA devices; include them in one Region; and configure low bandwidth codec as Audio preference list for devices in that Region.  
[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/admin/9\\_1\\_1/ccmcfq/CUCM\\_BK\\_A34970C5\\_00\\_admin-guide-91/CUCM\\_BK\\_A34970C5\\_00\\_admin-guide-91\\_chapter\\_0111.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/9_1_1/ccmcfq/CUCM_BK_A34970C5_00_admin-guide-91/CUCM_BK_A34970C5_00_admin-guide-91_chapter_0111.html)

## Increasing Server Resources

If you have spare hardware capacity on your VM infrastructure, you can increase the CPU and memory resources allocated to Unified CM, IM&P and Expressway servers. To do this, you can turn off the server, change VM specs to higher values, and turn the server on again.

Typically, adding CPUs benefits Unified CM and IM&P servers, and increasing CPU and memory benefits Expressway.

- [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/cucm-vmware-support.html](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/cucm-vmware-support.html)
- [http://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/virtualization-cisco-unified-communications-manager.html](http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-unified-communications-manager.html)
- [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/virtualization-cisco-ucm-session-management-edition.html](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-session-management-edition.html)
- [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/uc\\_system/virtualization/virtualization-cisco-ucm-im-presence.html](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/uc_system/virtualization/virtualization-cisco-ucm-im-presence.html)

**NOTE:** Increasing vCPU/memory is not guaranteed to increase the capacity of Expressway. The Expressway capacity section in the Profile Assessment will assist in understanding the scale you can achieve.

---

## MRA Deployment Best Practice – Software Solution Line-up

We recommend these minimum 12.5.x versions for the best MRA performance and stability:

Unified CM	IM&P	Expressway	Jabber
12.5(SU2)	12.5(SU2)	12.5.6	12.8.0 or higher

If you need to use Unified CM/IM&P 11.5.x versions, use these minimum versions:

Unified CM	IM&P	Expressway	Jabber
11.5(SU7)	11.5(SU7)	12.5.6	12.8.0 or higher

### **Unified CM/IM&P 10.x is not recommended**

Version 10.x is not recommended to support MRA. Many significant performance and stability improvements are available in Unified CM versions 11.x and later, which address MRA deployment at higher scale.

## MRA Serviceability

You can monitor the MRA call-flows on Unified CM and IM&P servers using the RTMT tool.

### Counters

This section lists some of the useful counters that are available.

#### **Get the list of registered SIP Phones:**

RTMT->Device->Phone Summary->Registered SIP Phones (indirect count)

#### **Counters for Number of registered phones and number of active video calls:**

RTMT -> System -> Performance -> Cisco CallManager:

- RegisteredHardwarePhones
- VideoCallsActive

#### **Tomcat UDS Request counters (can be obtained for other web-apps as well)**

RTMT -> System -> Performance -> Cisco Tomcat Web Application:

- Errors -> cucm-uds
- Requests -> cucm-uds
- SessionActive -> cucm-uds

RTMT -> System -> Performance -> Cisco Tomcat Connector

#### **TFTP and HTTP counters**

RTMT -> System -> Performance -> Cisco TFTP:

- HttpRequests
- HttpRequestsAborted
- HttpRequestsNotFound
- Requests
- RequestsAborted
- RequestsNotFound

#### **SSO counters:**

RTMT -> System -> Performance -> SAML SSO:

- SAMLRequests

- 
- SAMLResponses

#### Alerts to be monitored:

RTMT -> System -> Tools -> Alert Central:

- NumberOfRegisteredPhonesDropped
- NumberOfRegisteredDevicesExceeded

#### IM&P counters:

- Cisco XCP CM (Connection Manager)
- Cisco XCP Web CM (Connection Manager)
- Cisco XCP Auth Component (Authentication Component)
- Cisco XCP JSM
- Cisco Client Profile Agent
- Cisco Tomcat Connector

## Metrics

Instructions about how to configure Expressway to collect system metrics are in the *Expressway Serviceability Guide* [https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Serviceability-Guide-X8-11-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Serviceability-Guide-X8-11-1.pdf)

You can deploy a custom script on Expressway to get a list of endpoints registered through an Expressway-E/Expressway-C pair. Instructions and an example script are provided in Appendix 1 Example Script to List MRA-Registered Devices.

You can report Jabber client metrics to the Cisco cloud using Jabber telemetry if this feature is configured in your deployment. The telemetry can be viewed in Control Hub. More details are in [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/jabber/12\\_8/cjab\\_b\\_feature-configuration-for-jabber-128/cjab\\_b\\_feature-configuration-for-jabber-128\\_chapter\\_0100.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/12_8/cjab_b_feature-configuration-for-jabber-128/cjab_b_feature-configuration-for-jabber-128_chapter_0100.html)

## Logs

This section lists logs that are useful for troubleshooting MRA issues.

### Unified CM – download the logs from RTMT

- Cisco Tomcat
- Cisco Tomcat Security Logs
- Cisco CallManager
- Cisco Tftp
- Cisco User Data Services
- Cisco SSO
- Cisco Audit Logs
- Cron Logs
- Event Viewer-Application
- Event Viewer-System

### IM&P

- Client profile agent
- Cisco XCP authentication
- Cisco Tomcat security
- Cisco XCP Router
- Cisco XCP CM
- Cisco Presence Engine
- Cisco Intercluster sync agent
- Cisco AXL web service
- Cisco Tomcat
- Event Viewer – Application
- Event Viewer – System

### Expressway

The *Mobile and Remote Access Through Cisco Expressway Deployment Guide* has a troubleshooting chapter.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/expressway/config\\_guide/X12-](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-)

---

[5/exwy\\_b\\_mra-expressway-deployment-guide/exwy\\_b\\_mra-expressway-deployment-guide\\_chapter\\_01101.html](#)

You can deploy the Cisco Webex Serviceability Connector to make it easier and faster to enable, collect, and report the right logs to Cisco TAC when you need to report issues.

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cloudCollaboration/spark/hybridservices/serviceability/cmgt\\_b\\_deployment-guide-spark-hybrid-service-connector/cmgt\\_b\\_deployment-guide-spark-hybrid-service-connector\\_chapter\\_01.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cloudCollaboration/spark/hybridservices/serviceability/cmgt_b_deployment-guide-spark-hybrid-service-connector/cmgt_b_deployment-guide-spark-hybrid-service-connector_chapter_01.html)

## Appendix 1 Example Script to List MRA-Registered Devices

This Appendix describes how Expressway administrators can install and run a script to monitor the SIP connections on Expressway-E nodes. That is, to monitor the number of endpoints connected to the 5060/5061 port on Expressway-E at any point of time

### Example Script

**CAUTION:** The script illustrated here is an example only. The actual script requirements will depend on your specific deployment.

```
#!/usr/bin/env python

import os
import re
from datetime import datetime
import time

delay = 10
maxextsip = 0
while delay:
    netstat_output = os.popen("netstat -anp").readlines()
    now = datetime.now()
    currentsip = 0
    for line in netstat_output:
        localip, localport, fornip, fornport = "", "", "", ""
        localset, fornset = None, None
        fields = line.split()
        if len(fields) == 7:
            if fields[0] == 'tcp':
                local = fields[3].split(':')
                forn = fields[4].split(':')
                if len(local) == 2:
                    localset = 1
                    localip = local[0]
                    localport = local[1]
                if len(forn) == 2:
                    fornset = 1
                    fornip = forn[0]
                    fornport = forn[1]
            if localset and fornset:
                if re.search(r'506[0-1]', localport) or re.search(r'506[0-1]',
fornport):
                    if localip != "127.0.0.1" and fornip != "127.0.0.1" and forn-
nport != "0.0.0.0":
                        currentsip += 1
        if currentsip > maxextsip:
            maxextsip = currentsip
        dt_string = now.strftime("%d/%m/%Y %H:%M:%S")
        print('%s\tmax_ext_sip: %s current_ext_sip: %s' %
(dt_string,maxextsip,currentsip))
        time.sleep(delay)
```

---

## How to Configure

**Name of script:** ext\_sip.py

**Description:** A python script that counts the external SIP connections on Expressway-E port 5061/5060 in real time at 10s intervals. The script takes data based on running the '*netstat -anp*' command and counts external SIP connections. It runs this command every 10s and looks for the number of SIP connections.

### Procedure to Install and run:

Step 1: Copy the script (use scp) to /mnt/harddisk

```
Example: scp ext_sip.py root@<Exp-E IP>:/mnt/harddisk/ext_sip.py
```

Step 2: Make the script executable via the command 'chmod 777 <filename>'

Example:

```
~ # chmod 777 ext_sip.py
~ # ls -al ext_sip.py
-rwxrwxrwx 1 root root 1315 Mar 14 12:23 ext_sip.py
```

Step 3: Run the script

```
/mnt/harddisk # ./ext_sip.py
20/03/2020 07:33:42   max ext_sip: 2500 current ext_sip: 1500
20/03/2020 07:33:52   max ext_sip: 2500 current ext_sip: 1502
```

## Output Fields

The fields in the output include:

- Date in DD/MM/YYYY format
- Time: Expressway box time at the time of the run
- max\_ext\_sip: Indicates the maximum number of SIP connections seen on that box since the script was run.
- current\_ext\_sip: Indicates the number of SIP connections seen during that run.

**NOTE:** The ssh session (as root) to the Expressway has to be maintained to see the output. If the ssh session drops, the program will end and you will lose the 'max ext\_sip'.

## Appendix 2 Find List of Registered Devices - SOAP UI Tool and SXML API

### Reference Information

API Reference:- <https://developer.cisco.com/docs/sxml/#!risport70-api-reference/selectcmdevice>

### Procedure

Navigate to <https://<cucm-pub-ip>/realtimeservice2/>

1. Use the Unified CM administrator user id and password if you are prompted for credentials.
2. Click View Deployed Web Services.
3. Download the *RISService70 (WSDL)* - click the WSDL link and right-click "Save as".
4. Download the SOAP UI tool open source from this location:  
<https://www.soapui.org/downloads/soapui.html>
5. Open the SOAP UI tool and pass the WSDL to it.

---

## Example Request

This is a sample Request API that can be fed into the Soap UI tool.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:soap="http://schemas.cisco.com/ast/soap">
  <soapenv:Header/>
  <soapenv:Body>
    <soap:selectCmDevice>
      <soap:StateInfo></soap:StateInfo>
      <soap:CmSelectionCriteria>
        <soap:MaxReturnedDevices>1000</soap:MaxReturnedDevices>
        <soap:DeviceClass>Any</soap:DeviceClass>
        <soap:Model>30016</soap:Model>
        <soap:Status>Any</soap:Status>
        <soap:NodeName></soap:NodeName>
        <soap:SelectBy>Name</soap:SelectBy>
        <soap:SelectItems>
          <!--Zero or more repetitions:-->
          <soap:item>
            <soap:Item></soap:Item>
          </soap:item>
        </soap:SelectItems>
        <soap:Protocol>Any</soap:Protocol>
        <soap:DownloadStatus>Any</soap:DownloadStatus>
      </soap:CmSelectionCriteria>
    </soap:selectCmDevice>
  </soapenv:Body>
</soapenv:Envelope>
```

## Example Response

This is an extracted fragment from a sample Response to the previous example Request.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <ns1:selectCmDeviceResponse xmlns:ns1="http://schemas.cisco.com/ast/soap">
      <ns1:selectCmDeviceReturn>
        <ns1:SelectCmDeviceResult>
          <ns1:TotalDevicesFound>7</ns1:TotalDevicesFound>
          <ns1:CmNodes>
            <ns1:item>
              <ns1:ReturnCode>Ok</ns1:ReturnCode>
              <ns1:Name>10.106.211.102</ns1:Name>
              <ns1:NoChange>>false</ns1:NoChange>
              <ns1:CmDevices>
                <ns1:item>
                  <ns1:Name>abcd</ns1:Name>
                  <ns1:DirNumber>1030-UnRegistered</ns1:DirNumber>
                  <ns1:DeviceClass>Phone</ns1:DeviceClass>
                  <ns1:Model>30016</ns1:Model>
                  <ns1:Product>30041</ns1:Product>
                  <ns1:BoxProduct>0</ns1:BoxProduct>
                  <ns1:Httpd>Yes</ns1:Httpd>
                  <ns1:RegistrationAttempts>0</ns1:RegistrationAttempts>
                  <ns1:IsCtiControllable>>true</ns1:IsCtiControllable>
                  <ns1:LoginUserId xsi:nil="1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"/>
                  <ns1>Status>UnRegistered</ns1>Status>
                  <ns1>StatusReason>10</ns1>StatusReason>
                  <ns1:PerfMonObject>2</ns1:PerfMonObject>
                  <ns1:DChannel>0</ns1:DChannel>
                </ns1:item>
              </ns1:CmDevices>
            </ns1:item>
          </ns1:CmNodes>
        </ns1:SelectCmDeviceResult>
      </ns1:selectCmDeviceReturn>
    </ns1:selectCmDeviceResponse>
  </soapenv:Body>
</soapenv:Envelope>
```

---

```
        <ns1:Description>Auto 1030</ns1:Description>
        <ns1:H323Trunk>
...
...
...
        <ns1:IPAddress>
            <ns1:item>
                <ns1:IP>192.168.43.26</ns1:IP>
                <ns1:IPAddrType>ipv4</ns1:IPAddrType>
                <ns1:Attribute>Unknown</ns1:Attribute>
            </ns1:item>
        </ns1:IPAddress>
    </ns1:item>
</ns1:CmDevices>
</ns1:item>
</ns1:CmNodes>
</ns1>SelectCmDeviceResult>
    <ns1:StateInfo>&lt;StateInfo ClusterWide="1"&lt;Node
Name="10.106.211.102" SubsystemStartTime="1583491640" StateId="688"
TotalItemsFound="7" TotalItemsReturned="7"/&lt;/StateInfo></ns1:StateInfo>
    </ns1:selectCmDeviceReturn>
</ns1:selectCmDeviceResponse>
</soapenv:Body>
</soapenv:Envelope>
```