



# Cisco Mobile and Remote Access Best Practices for Optimizing Scale

## Application Note

September 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
Optimizing Existing Deployments for Increased MRA Use .....	6
Release Keys, Option Keys, and General Licensing.....	6
Optimizing Sign In--LDAP, UDS and Authentication.....	7
Optimizing Sign In--MRA IM&P Inter Cluster Synch Agent Dependency .....	8
Optimizing Resource Consumption on Unified CM and Expressway .....	9
Optimizing Resource Consumption During IM&P Processing .....	10
Optimizing Traffic .....	11
Increasing Server Resources.....	12
Optimizing the Security Posture of MRA Deployments .....	12
MRA Deployment Best Practice – Software Solution Line-up .....	12
MRA Serviceability.....	13
Counters.....	13
Metrics.....	14
Logs.....	15
Appendix 1 Example Script to List MRA-Registered Devices (Not Needed from X12.6.1) .....	16
Appendix 2 Find List of Registered Devices – SOAP UI Tool and SXML API .....	18

## Purpose of this Document

COVID-19 is causing an unprecedented challenge for customers to support increasing number of employees working from home. Existing customer solutions are typically architected to host a much lower percentage of employees working from home than is now required.

Cisco Unified Communications customers with Cisco Jabber can leverage standard VPN options to the home. Cisco also supports VPN-less access, through our Unified Communications Mobile and Remote Access (MRA) service.

This note summarizes the following information for MRA-based deployments:

- Best practices and short-term measures to optimize **existing** capacity to support increased MRA use. Pointers about system monitoring and troubleshooting, and links to customer support documents.
- Recommendations for how to assess and plan for adding **new** capacity.

## MRA Overview

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. The Cisco Expressway Series product (Expressway) provides secure firewall traversal and line-side support for Unified CM registrations.

More details about MRA are available 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/X12-6/exwvy\\_b\\_mra-expressway-deployment-guide.pdf](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-6/exwvy_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 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/X12-6/Cisco-Expressway-Cluster-Creation-and-Maintenance-Deployment-Guide-X12-6.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-6/Cisco-Expressway-Cluster-Creation-and-Maintenance-Deployment-Guide-X12-6.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.**

---

## Optimizing 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.

**Note:** These recommendations generally apply to Cisco Jabber soft clients and other endpoints that are compatible with MRA. For IM&P, they apply only to Jabber clients.

## Release Keys, Option Keys, and General Licensing

- Cisco Expressway Series (Expressway) products do not need a release key to upgrade a system on X8.6.x or later software to X12.6 or later.
- Smart Licensing is available from X12.6 for Expressway products.
- Option keys were previously used to configure the **Series** for a system ("Cisco Expressway Series" or "Cisco VCS") and its **Type** ("-E" or "-C" role). These functions are now managed through web UI settings, and the option keys concerned are no longer used from X12.6.  
[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/release\\_note/Cisco-Expressway-Release-Note-X12-6.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/release_note/Cisco-Expressway-Release-Note-X12-6.pdf)

## Optimizing Sign In--LDAP, UDS and Authentication

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

- Use OAuth refresh (self-describing tokens) sign in flow to avoid the need for Expressway to contact Unified CM to validate the access token presented by the client. This can be used with SSO-based signin or with LDAP (also with local Unified CM end user accounts).  
[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 describing 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 use OAuth refresh (self-describing tokens) sign in flow, it is possible, although 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.

**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)

- To allow Jabber clients to take advantage of the UDS bulk query feature, upgrade to Unified CM version 11.5(SU7) or 12.5(SU2), and to Jabber version 12.8.0 or higher.
- If you notice that Expressway MRA performance is impacted at certain hours of the day, explore the possibility of users signing in in shifts, with a 15-minute offset.
- Perform Unified CM upgrades during lean times, so that bulk Jabber signins/failovers do not occur. Expect longer re-signin times when there are network outages.
- To avoid email-based lookups by Jabber clients (which are performed individually rather than in batches) we recommend setting the Directory URI attributes for LDAP as follows:
  - Directory URI on Unified CM LDAP to *msRTCSIP-primaryuseraddress*.
  - Directory URI attribute on the Unified CM LDAP Directory page to the *msRTCSIP-primaryuseraddress* attribute in AD.
- 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. 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. The *Callhistory\_Expire\_Days* parameter lets you specify the number of days before the call history is deleted. The maximum number of call records stored is 250. If the value is zero or not specified, the call history stores the maximum number of records (250).

Example: `<Callhistory_Expire_Days>2</Callhistory_Expire_Days>` stores the call history for a maximum of 2 days.

## Optimizing Sign In--MRA IM&P Inter Cluster Synch Agent Dependency

These are some pointers to ensure that deployments with multiple IM&P clusters have Inter Cluster Synch Agent (ICSA) enabled and functioning correctly:

- If IM&P services are required by a Jabber client, failure to sign into IM&P services over MRA may cause complete MRA Jabber signin 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.



## Optimizing 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\\_CEF360A6\\_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_CEF360A6_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. (Typically, third party or custom configuration tools use AXL to talk to Unified CM.) The method to do this will depend on the specific tools in use for your deployment.
- 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 Cisco CallManager services on the Unified CM Publisher node if your Expressway version is X12.5.7 or higher.
- Expressway X12.6.1 includes the fix for Bug ID [CSCvt55506](#) *Socket process causing High CPU*. If you previously implemented the workaround for this bug, you can if you wish now reconfigure the Sockhandler to use EPOLL mode again. The commands to do this are:
  - *xConfiguration Sockhandler EPOLL Mode: "On"*
  - *xCommand Restart*

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/release\\_note/Cisco-Expressway-Release-Note-X12-6-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/release_note/Cisco-Expressway-Release-Note-X12-6-1.pdf)

---

## Optimizing 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. To disable Click2X, administrators can use the following methods:
  - Push a reinstallation of Jabber with the correct install parameters, as detailed in the guide below.
  - Push an updated *jabber-bootstrap.properties* file to this location: *C:\ProgramData\Cisco Systems\Cisco Jabber*  
The updated file would include the line: "Click2XEnabled: Disabled". This line can be placed anywhere in the file.  
[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)
- Android PUSH for IMP over MRA is disabled by default in X12.6.2. This is due to unexpected results for deployments that use Cisco Jabber for Android 12.9 or later (bug ID [CSCw12541](#)).  
[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/release\\_note/Cisco-Expressway-Release-Note-X12-6-2.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/release_note/Cisco-Expressway-Release-Note-X12-6-2.pdf)

## Optimizing 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 is to be turned off. The configured bandwidth limit should allow only audio calls ( $\leq 128$  kbps).

Configure the Region setting for device groups and set **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/12\\_5\\_1SU2/systemConfig/cucm\\_b\\_system-configuration-guide-1251su2/cucm\\_b\\_system-configuration-guide-for-cisco-1251su2\\_chapter\\_0111.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU2/systemConfig/cucm_b_system-configuration-guide-1251su2/cucm_b_system-configuration-guide-for-cisco-1251su2_chapter_0111.html)

- You can configure PSTN fallback 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).
- 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.
  - Processing by Expressway and the bandwidth consumed for Internet connectivity from your data center, is limited.

ICE Passthrough is available from versions 12.5 and above for Unified CM and Expressway.

[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 the 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/12\\_5\\_1SU2/systemConfig/cucm\\_b\\_system-configuration-guide-1251su2/cucm\\_b\\_system-configuration-guide-for-cisco-1251su2\\_chapter\\_0111.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1SU2/systemConfig/cucm_b_system-configuration-guide-1251su2/cucm_b_system-configuration-guide-for-cisco-1251su2_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.

## Optimizing the Security Posture of MRA Deployments

Expressway TURN does not operate as a STUN server. Due to security enhancements in X12.6.1, the Expressway-E TURN server no longer functions as a generic STUN server and will not accept unauthenticated STUN binding requests. This enhances the security posture for ICE over MRA deployments.

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/release\\_note/Cisco-Expressway-Release-Note-X12-6-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/release_note/Cisco-Expressway-Release-Note-X12-6-1.pdf)

## 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)	X12.5.6	12.8.0 or higher
12.5(SU3)	12.5(SU3)	X12.6 / X12.6.1	12.9

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)	X12.5.6	12.8.0 or higher

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

Version 10.x is not recommended for 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 useful counters that are available.

#### Get list of registered SIP phones

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

**From Expressway-E:** Active MRA Registrations count on **Status > Overview** page - **MRA Registrations** section. Shows count of current active MRA devices and peak count for MRA registrations since last Expressway restart.

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/release\\_note/Cisco-Expressway-Release-Note-X12-6-1.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/release_note/Cisco-Expressway-Release-Note-X12-6-1.pdf)

#### 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 Administrator Guide*, section “System Metrics Collection”

[https://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/expressway/admin\\_guide/Cisco-Expressway-Administrator-Guide-X12-6-2.pdf](https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/expressway/admin_guide/Cisco-Expressway-Administrator-Guide-X12-6-2.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
- Cisco Tomcat security
- Cisco XCP Router
- Cisco XCP CM
- Cisco Presence Engine
- Cisco Intercluster sync agent
- Cisco AXL web service
- 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/X12-6/exwy\\_b\\_mra-expressway-deployment-guide/exwy\\_b\\_mra-expressway-deployment-guide\\_chapter\\_01101.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/expressway/config_guide/X12-6/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 (Not Needed from X12.6.1)

**This script is not needed on Expressways that are running version X12.6.1 or later**, as MRA registration counters are available on Expressway-E from X12.6.1.

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 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 for-
nport != "0.0.0.0":
                        currentsip += 1
        if currentsip > maxextsip:
            maxextsip = currentsip
```



---

Appendix 1 Example Script to List MRA-Registered Devices (Not Needed from X12.6.1)

```
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 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 must 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: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>
```