MRA Troubleshooting

General Techniques

Alarms and Status Messages

When troubleshooting, first check if any alarms have been raised (**Status** > **Alarms**). If alarms exist, follow the instructions in the **Action** column. Check the alarms on both Cisco Expressway-C and Cisco Expressway-E.

Next, review the status summary and configuration information (**Status** > **Unified Communications**). Check the status page on both Cisco Expressway-C and Cisco Expressway-E. If any required configuration is missing or invalid, an error message and a link to the relevant configuration page is shown.

You may see invalid services or errors if you change the following items on Cisco Expressway, for which a system restart is required to be sure the configuration changes take effect:

- Server or CA certificates
- DNS configuration
- Domain configuration

Use the Collaboration Solutions Analyzer

The Collaboration Solutions Analyzer (CSA) tool set provided by TAC, can be used to help with deploying and troubleshooting MRA. (See the Cisco Expressway release notes for instructions about how to access the CSA.)

Step 1 Use the CollabEdge **validator tool** to validate your MRA deployment.

It simulates a Jabber client sign in process and provides feedback on the result.

Step 2 If the CollabEdge validator cannot identify the issue, we suggest that you collect logs from the Cisco Expressway while attempting to sign in. Then use the **log analysis** component in the CSA to analyze the logs.

Diagnostic Logs

Jabber for Windows Diagnostic Logs

The Jabber for Windows log file is saved as `csf-unified.log` under `C:\Users\<UserID>\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`.

Configure Cisco Expressway Diagnostic Log Levels

The diagnostic logging tool in Cisco Expressway can be used to assist in troubleshooting system issues. It allows you to generate a diagnostic log of system activity over a period and then to download the log.

Before you begin

Before taking a diagnostic log, you must configure the log level of the relevant logging modules.

Step 1 Go to **Maintenance** > **Diagnostics** > **Advanced** > **Support Log configuration**.

Step 2 Select the recommended logs for the problem you are experiencing. You can find these using the Log Advisor Tool: https://logadvisor.cisco.com/logadvisor/collaboration/unifiedcommunications/mra.

Step 3 Click **Set to debug**.

Create a Diagnostic Log Capture

After you configure the Cisco Expressway diagnostic log levels, you can start the diagnostic log capture.

Step 1 Go to **Maintenance** > **Diagnostics** > **Diagnostic logging**.

Step 2 (Optional) Select **Take tcpdump while logging**.

Step 3 Click **Start new log**.

Step 4 (Optional) Enter some **Marker** text and click **Add marker**.

- The marker facility can be used to add comment text to the log file before certain activities are performed. This helps to subsequently identify the relevant sections in the downloaded diagnostic log file.
- You can add as many markers as required, at any time while the diagnostic logging is in progress.
- Marker text is added to the log with a "**DEBUG_MARKER**" tag.

Step 5 Reproduce the system issue you want to trace in the diagnostic log.

Step 6 Click **Stop logging**.

Step 7 Click **Collect log**.

Step 8 When the log collection completes, click **Download log** to save the diagnostic log archive to your local file system.

You are prompted to save the archive (the exact wording depends on your browser).

After You Create Logs

If you want to download the logs again, you can re-collect them by using the **Collect log** button. If the button is grayed out, first refresh the page in your browser.

After you have completed your diagnostic logging, return to the **Support Log configuration** page and reset the modified logging modules back to *INFO* level.

Check DNS Records

You can use the Cisco Expressway's DNS lookup tool to assist in troubleshooting system issues.

Go to **Maintenance** > **Tools** > **Network utilities** > **DNS lookup**.

The SRV record lookup includes those specific to H.323, SIP, Unified Communications and TURN services.

Note Performing the DNS lookup from the Cisco Expressway-C returns the view from within the enterprise, and that performing it on the Cisco Expressway-E returns what is visible from within the DMZ which is not necessarily the same set of records available to endpoints in the public internet.

The DNS lookup includes the following SRV services that are used for Unified Communications:

- _collab-edge._tls
- _cisco-uds._tcp

Check that the Cisco Expressway-E is Reachable

This procedure describes how to check that the Cisco Expressway-E is reachable.

Ensure that the FQDN of the Cisco Expressway-E is resolvable in the public DNS.

The FQDN is configured at **System** > **DNS** and is built as **<System host name>.<Domain name>**.

Check Call Status

Call status information can be displayed for both current and completed calls.

The same set of call status information is also shown on the **Calls by registration** page (accessed via the **Registration details** page).

If the Cisco Expressway is part of a cluster, all calls that apply to any peer in the cluster are shown, although the list is limited to the most recent 500 calls per peer.

Step 1 If you wish to get information about the current calls, go to the **Call status** page (**Status** > **Calls** > **Calls**).

The **Call status** page lists all the calls currently taking place to or from devices registered with the Cisco Expressway, or that are passing through the Cisco Expressway.

Step 2 If you wish to get information about the completed calls, go to the **Call history** page (**Status** > **Calls** > **History**).

The **Call history** page lists all the calls that are no longer active. The list is limited to the most recent 500 calls, and only includes calls that have taken place since the Cisco Expressway was last restarted.

Mobile and Remote Access Call Identification

The call status and call history pages show all call types—Unified CM remote sessions (if Mobile and Remote Access is enabled) as well as Cisco Expressway RMS sessions.

To distinguish between the call types, you must drill down into the call components. Mobile and Remote Access calls have different component characteristics depending on whether the call is being viewed on the Cisco Expressway-C or Cisco Expressway-E:

- On the Cisco Expressway-C, a Unified CM remote session has three components (as it uses the B2BUA to enforce media encryption). One of the Cisco Expressway components routes the call through one of the automatically generated neighbor zones (with a name prefixed by either **CEtcp** or **CEtls**) between Cisco Expressway and Unified CM.
- On the Cisco Expressway-E, there is one component and that routes the call through the **CollaborationEdgeZone**.

If both endpoints are outside of the enterprise (that is, off premises), you will see this treated as two separate calls.

Rich Media Sessions (Cisco Expressway Only)

If your system has a rich media session key installed and thus supports business-to-business calls, and interworked or gatewayed calls to third-party solutions and so on, those calls are also listed on the call status and call history pages.

Devices Registered to Unified CM via Cisco Expressway

Identify Devices in Unified CM

This procedure describes how to identify devices registered to Unified CM via Cisco Expressway.

Step 1 In Unified CM, go to **Device** > **Phone** and click **Find**.

Step 2 Check the **IP Address** column.

Devices that are registered via Cisco Expressway will display the IP Address of the Cisco Expressway-C it is registered through.

Identify Provisioning Sessions in Cisco Expressway-C

This procedure describes how to identify sessions that have been provisioned via Cisco Expressway-C.

Step 1 In Cisco Expressway-C, go to **Status** > **Unified Communications**.

Step 2 In the **Advanced status information** section, click **View provisioning sessions**.

This shows a list of all current and recent (shown in red) provisioning sessions.

Ensure that Cisco Expressway-C is Synchronized to Unified CM

Changes to Unified CM cluster or node configuration can lead to communication problems between Unified CM and Cisco Expressway-C. This includes changes to the following items:

- Number of nodes within a Unified CM cluster
- Host name or IP address of an existing node
- Listening port numbers
- Security parameters
- Phone security profiles

You must ensure that any such changes are reflected in the Cisco Expressway-C. To do this:

Step 1 On Cisco Expressway, go to **Configuration** > **Unified Communications**.

Step 2 Rediscover all Unified CM and IM and Presence Service nodes.

Check MRA Authentication Status and Tokens

This procedure describes how to check MRA authentication status and tokens.

Step 1 (Optional) To check and clear standard (non-refresh) OAuth user tokens, go to **Users** > **View and manage OAuth without refresh token holders**.

This could help identify problems with a particular user's OAuth access.

Step 2 (Optional) To check statistics for MRA authentication, go to **Status** > **Unified Communications** > **View detailed MRA authentication statistics**.

Any unexpected requests or responses on this page could help identify configuration or authorization issues.

Registration Issues

Endpoints Can't Register to Unified CM

Endpoints may fail to register for various reasons:

- Endpoints may not be able to register to Unified CM if there is also a SIP trunk configured between Unified CM and Cisco Expressway-C. If a SIP trunk is configured, you must ensure that it uses a different listening port on Unified CM from that used for SIP line registrations to Unified CM. See SIP Trunks Between Unified CM and Expressway-C for more information.
- Secure registrations may fail ('`Failed to establish SSL connection`' messages) if the server certificate on the Cisco Expressway-C does not contain in its Subject Alternate Name list, the names of all of the Phone Security Profiles in Unified CM that are configured for encrypted TLS and are used for devices requiring remote access. Note that these names — in both Unified CM and in the Cisco Expressway's certificate — must be in FQDN format.

  It is essential to generate Certificate Signing Request (CSR) for the new node while adding a new Expressway-C node to an existing cluster of Expressway-C. It is mandated to put secure profile names as they are on CUCM, if secure registration of Mobile and Remote Access (MRA) client is needed over MRA. CSR creation on the new node will fail if “Unified CM phone security profile names” are just names or hostnames on CUCM device security profiles. This will force Administrators to change the value of “Unified CM phone security profile names” on CUCM under the **Secure Phone Profile** page.

  From X12.6, it is mandated that the Unified CM phone security profile name must be a Fully Qualified Domain Name (FQDN). It cannot be just any name or hostname or a value.

  For example, `jabbersecureprofile.domain.com`, `DX80SecureProfile.domain.com`

Note The FQDN can comprise multiple levels. Each level's name can only contain letters, digits, and hyphens, with each level separated by a period (dot). A level name cannot start or end with a hyphen, and the final level name must start with a letter.

Cisco Expressway Certificate and TLS Connectivity Issues

Modifications to the Cisco Expressway's server certificate or trusted CA certificates need a Cisco Expressway restart for the changes to take effect.

If you are using secure profiles, ensure that the root CA of the authority that signed the Cisco Expressway-C certificate is installed as a CallManager-trust certificate (**Security** > **Certificate Management** in the **Cisco Unified OS Administration** application).

CiscoSSL 5.4.3 Rejects Diffie-Hellman Keys with Fewer than 1024 Bits

If you are running version 9.x, or earlier, of Unified CM or Unified CM IM and Presence Service, with Cisco Expressway version X8.7.2 or later, then the SSL handshake between the two systems will fail by default.

The symptom is that all MRA endpoints fail to register or make calls after you upgrade to Cisco Expressway X8.7.2 or later.

The cause of this issue is an upgrade of the CiscoSSL component to 5.4.3 or later. This version rejects the default (768 bit) key provided by Unified CM when using D-H key exchange.

You must either upgrade your infrastructure or consult the Cisco Technical Assistance Center to check whether it is possible to modify the default configurations for Unified CM and/or Unified CM IM and Presence Service to support TLS (refer CSCuy59366).

Cisco Jabber Sign In Issues

Jabber Triggers Automated Intrusion Protection

Conditions

- Your MRA solution is configured for authorization by OAuth token (with or without refresh)
- The Jabber user's access token has expired
- Jabber does one of these:
  - Resumes from desktop hibernate
  - Recovers network connection
  - Attempts fast login after it has been signed out for several hours

Behavior

- Some Jabber modules attempt to authorize at Cisco Expressway-E using the expired access token.
- The Cisco Expressway-E (correctly) denies these requests.
- If there are more than 5 such requests from a particular Jabber client, the Cisco Expressway-E blocks that IP address for ten minutes (by default).

Symptoms

The affected Jabber clients' IP addresses are added to the Cisco Expressway-E's **Blocked addresses** list, in the *HTTP proxy authorization failure* category. You can see these on **System** > **Protection** > **Automated detection** > **Blocked addresses**.

Workaround

There are two ways you can work around this issue; you can increase the detection threshold for that particular category, or you can create exemptions for the affected clients. We describe the threshold option here because the exemptions may well be impractical in your environment.

1. Go to **System** > **Protection** > **Automated detection** > **Configuration**.
2. Click **HTTP proxy authorization failure**.
3. Change the **Trigger level** from *5* to *10*. 10 should be enough to tolerate the Jabber modules that present expired tokens.
4. Save the configuration, which takes effect immediately.
5. Unblock any affected clients.

Jabber Popup Warns About Invalid Certificate When Connecting from Outside the Network

This is a symptom of an incorrectly configured server certificate on the Cisco Expressway-E. The certificate could be self-signed, or it may not have the external DNS domain of your organization listed as a subject alternative name (SAN).

This is expected behavior from Jabber. We recommend that you install a certificate issued by a CA that Jabber trusts, and that the certificate has the domains Jabber is using included in its list of SANs. See Certificate Requirements.

Jabber Doesn't Register for Phone Services

There is a case handling mismatch between the Cisco Expressway and the User Data Service (UDS) that prevents Jabber from registering for phone services if the supplied user ID does not match the case of the stored ID. Jabber still signs in but cannot use phone services.

Users can avoid this issue by signing in with the user ID exactly as it is stored in UDS.

Users can recover from this issue by signing out and resetting Jabber. See CSCux16696.

Jabber Cannot Sign in Due to XMPP Bind Failure

The Jabber client may be unable to sign in ("Cannot communicate with the server" error messages) due to XMPP bind failures.

This will be indicated by resource bind errors in the Jabber client logs, for example:

```
XmppSDK.dll #0, 201, Recv:<iq id='uid:527a7fe7:00000cfe:00000000' type='error'><bind
xmlns='urn:ietf:params:xml:ns:xmpp-bind'/><error code='409' type='cancel'><conflict
xmlns='urn:ietf:params:xml:ns:xmpp-stanzas'/></error></iq>

XmppSDK.dll #0, CXmppClient::onResourceBindError

XmppSDK.dll #0, 39, CTriClient::HandleDisconnect, reason:16
```

This typically occurs if the IM and Presence Intercluster Sync Agent is not working correctly. See IM and Presence information in the *Cisco Unified Communications Manager Configuration Guides* at

https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-installation-and-configuration-guides-list.html.

Jabber Cannot Sign in Due to SSH Tunnels Failure

Jabber can fail to sign in due to the SSH tunnels failing to be established. The traversal zone between the Cisco Expressway-C and Cisco Expressway-E will work normally in all other respects. Cisco Expressway will report '`Application failed - An unexpected software error was detected in portforwarding.pyc`'.

This can occur if the Cisco Expressway-E DNS hostname contains underscore characters. Go to **System** > **DNS** and ensure that the **System host name** only contains letters, digits, and hyphens.

Jabber Cannot Sign in When Connecting to Different Peers in a Cluster of Cisco Expressway-Es

Jabber sign in failures have been seen when there is inconsistency of the DNS domain name between Cisco Expressway-E peers. The domain names must be identical, even with respect to case, on all peers in the cluster.

Go to **System** > **DNS** on each peer to make sure that Domain name is identical on all peers.

Specific Issues

Cisco Expressway Returns “401 Unauthorized” Failure Messages

A “401 Unauthorized” failure message can occur when the Cisco Expressway attempts to authenticate the credentials presented by the endpoint client. The reasons for this include:

- Note that the solution must be configured to userid of the IDP that is provided in the SAML assertion should match the sAMAccountName of CUCM userid to validate against the tokens (access/refresh).
- The client is supplying an unknown username or the wrong password.
- Intercluster Lookup Service (ILS) has not been set up on all the Unified CM clusters. This may result in intermittent failures, depending upon which Unified CM node is being used by Cisco Expressway for its UDS query to discover the client's home cluster.

Call Failures due to “407 Proxy Authentication Required” or “500 Internal Server Error” Errors

Call failures can occur if the traversal zones on Cisco Expressway are configured with an **Authentication policy** of *Check credentials*. Ensure that the **Authentication policy** on the traversal zones used for Mobile and Remote Access is set to *Do not check credentials*.

Call Bit Rate is Restricted to 384 kbps or Video Issues when Using BFCP (Presentation Sharing)

This can be caused by video bit rate restrictions within the regions configured on Unified CM.

Ensure that the **Maximum Session Bit Rate for Video Calls** between and within regions (**System** > **Region Information** > **Region**) is set to a suitable upper limit for your system, for example 6000 kbps.

IM and Presence Service Realm Changes

Provisioning failures can occur when the IM and Presence Service realm has changed and the realm data on the Cisco Expressway-C has not been updated.

For example, this could happen if the address of an IM and Presence Service node has changed, or if a new peer has been added to an IM and Presence Service cluster.

The diagnostic log may contain an INFO message like "`Failed to query auth component for SASL mechanisms`" because the Cisco Expressway-C cannot find the realm.

Go to **Configuration** > **Unified Communications** > **IM and Presence Service nodes** and click **Refresh servers** and then save the updated configuration. If the provisioning failures persist, verify the IM and Presence Service nodes configuration and refresh again.

No Voicemail Service ("403 Forbidden" Response)

Ensure that the Cisco Unity Connection (CUC) hostname is included on the HTTP server allow list on the Cisco Expressway-C.

"403 Forbidden" Responses for Any Service Requests

Services may fail ("403 Forbidden" responses) if the Cisco Expressway-C and Cisco Expressway-E are not synchronized to a reliable NTP server. Ensure that all Cisco Expressway systems are synchronized to a reliable NTP service.

Client HTTPS Requests are Dropped by Cisco Expressway

This can be caused by the automated intrusion protection feature on the Cisco Expressway-E if it detects repeated invalid attempts (404 errors) from a client IP address to access resources through the HTTP proxy.

To prevent the client address from being blocked, ensure that the **HTTP proxy resource access failure** category (**System** > **Protection** > **Automated detection** > **Configuration**) is disabled.

Failed: Address is not a IM and Presence Server

This error can occur when trying to configure the IM and Presence Service servers used for remote access (via **Configuration** > **Unified Communications** > **IM and Presence servers**). It is due to missing CA certificates on the IM and Presence Service servers and applies to systems running 9.1.1. More information and the recommended solution is described in CSCul05131.

Invalid SAML Assertions

If clients fail to authenticate via SSO, one potential reason is that invalid assertions from the IDP are being rejected by the Cisco Expressway-C.

Check the logs for `Invalid SAML Response`.

One example is when ADFS does not have a claim rule to send the users' IDs to the Cisco Expressway-C. In this case you will see `No uid Attribute in Assertion from IdP` in the log.

The Cisco Expressway is expecting the user ID to be asserted by a claim from ADFS that has the identity in an attribute called **`uid`**. You need to go into ADFS and set up a claim rule, on each relying party trust, to send the users' AD email addresses (or sAMAccountNames, depending on your deployment) as “uid” to each relying party.

“502 Next Hop Connection Failed” Messages

A 502 message on the Cisco Expressway-E indicates that the next hop failed (typically to the Cisco Expressway-C). Try the following steps:

1. Go to the **Status** > **Unified Communications** page on the Cisco Expressway-E. Did the Cisco Expressway-E report any issues?
2. If the status looks normal, click the **SSH tunnel status** link at the foot of the status page. If one or more tunnels to the Cisco Expressway-C node is down, that is probably causing the 502 error.

MRA calls fail if the called endpoint is more than 15 hops away from the Expressway-E

The Unified Communications traversal zone has a default hop count of 15. If you suspect this is a contributing factor, sign in to all your MRA Expressways, raise the hop count to a significantly larger number, for example, 70 and test.

MRA calls fail if the called endpoint is more than 15 hops away from the Expressway-E