Troubleshoot Jabber Log in Problems

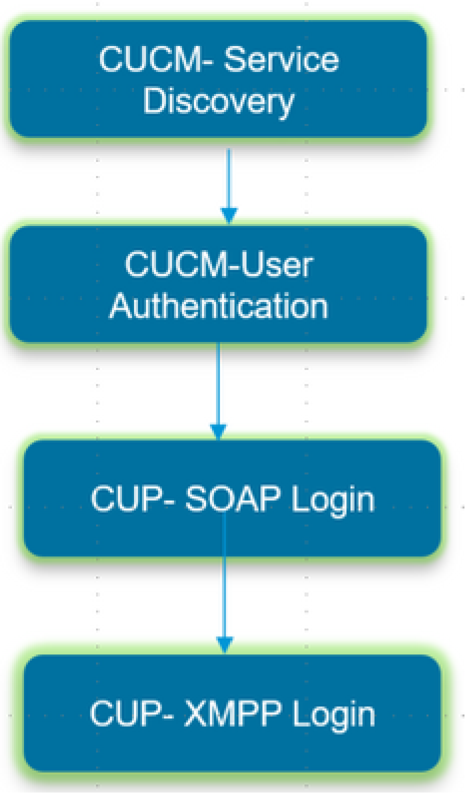
Contents

Introduction

This document describes how to troubleshoot the Jabber Log in when it fails on an internal or corporate network.

Background Information

Jabber Log in comprises of two stages; Cisco Unified Communications Manager server (CUCM) Log in and IM and Presence server (IM&P) Log in.



- CUCM Log in involves Service discovery to identify the CUCM server to which Jabber must log in.

- Jabber uses Authentication with CUCM to retrieve the Service profile details which contains IMP server, Voicemail, Conferencing, CTI server details and also Device Configuration file for Phone services.

- Once the CUCM Log in is successful, Jabber logs in to the IMP server to authenticate and retrieve the contact list and other IM services.

- The IMP Log in has two stages namely: SOAP Log in which deals with user authentication, and then XMPP Log in which deals with XMPP session creation and Stream Management.

How to Collect Logs

Clear the cache on the PC and collect the clean Jabber Problem Report (PRT).

Step 1. Sign out and exit the Jabber application.
Step 2. Delete all the logs located at

> **%AppData%\Local\Cisco\Unified Communications\Jabber\**
> **%AppData%\Roaming\Cisco\Unified Communications\Jabber\**

Step 3. Restart Jabber and recreate the problem.

Step 4. Collect the Problem report. (From the Jabber **Help menu**, select **Report a problem** option to launch the problem report tool. The instructions are found there)

Link to these resources:

- How to collect a Jabber Problem
- How to collect logs from Expressway (When Jabber is over MRA)

Keywords to Search in Logs

<#root>

```
IMPStackCap::Log in::OnLog inError
ServiceDiscoveryHandlerResult
@CupSoapCli: log in cup succeeds -
```

shows when the SOAP log in was successful.

```
[CTriTPConnectionClient::OnConnectSuccess] - @XmppSDK: -
```

shows when the XMPP log in was successful.

```
LERR -
```

shows the Log in Errors when the Jabber fails to log in to the IM&P Server.

Stages to Troubleshoot

Stage 1. CUCM Service Discovery

Error on screen	Cause	What to check in Jabber log
Cannot find your services automatically. Click Advanced settings to set up manually	This error is seen when the **_cisco-uds** or _cuplog in SRV records are not configured in the DNS server	csf::dns::mapFromWindowsDNSResult

Sample Log Snippet

<#root>

```
017-03-19 17:55:00,422 WARN  [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns]   [csf::dns::mapFromWindowsDNSResult] - *-----*

DNS query _cisco-uds._tcp.applab has failed

:

 DNS name does not exist.  (9003).

2017-03-19 17:55:00,438 WARN  [0x000050ac] [src\dnsutils\win32\win32DnsUtils.cpp(52)] [csf.dns]   [csf::

DNS query _cuplogin._tcp.applab has failed

: DNS name does not exist. (9003).
```

Steps to Resolve

Step 1. Start the command prompt (on a Windows Client) and then enter **nslookup**.

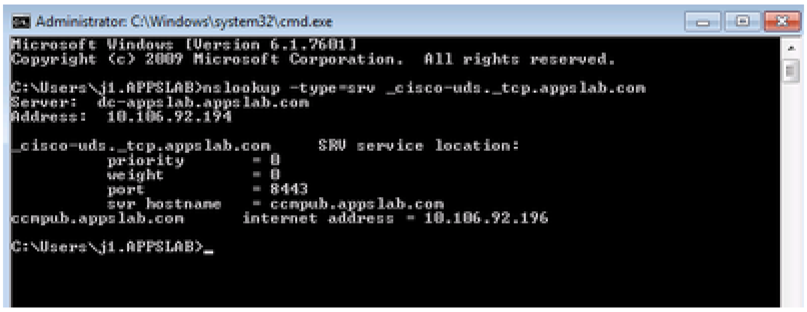
Step 2. Set the query type to SRV
set type = SRV

Step 3. Insert the SRV record we need to check
_cisco-uds._tcp.example.com

Step 4. This returns the DNS A records which point to the CUCM servers.

This is an example of the Successful _cisco-uds SRV record.

If no records are returned, contact your DNS administrator to configure the SRV records



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\j1.APPSLAB>nslookup -type=srv _cisco-uds._tcp.appslab.com
Server:  dc-appslab.appslab.com
Address:  10.106.92.194

_cisco-uds._tcp.appslab.com     SRV service location:
          priority       = 0
          weight         = 0
          port           = 8443
          svr hostname   = ccmpub.appslab.com
ccmpub.appslab.com      internet address = 10.106.92.196

C:\Users\j1.APPSLAB>_
```

Error on screen	Cause	What to check in Jabber log
Cannot find your services automatically. Click Advanced settings to set up manually	This error is seen when the **Jabber** is unable to retrieve the UDS or TFTP Servers to gather its log in information and configuration settings.	HTTP response code 503 for request #29 to https://cucm.domain:8443/cucm-uds/ HTTP response code 503 for request #29 to https://cucm.domain:6972/

Steps to Resolve

Step 1. Validate that the CUCM nodes configured as TFTP Servers are up and running.

Step 2. **Restart** these services on all the CUCM nodes.

- **Cisco TFTP**
- **Cisco UDS Service**

Stage 2. CUCM User Authentication

Error on screen	Cause	What to check in Jabber log
Your username or password is not correct	This error is seen when the credentials entered is wrong or the user is locked in CUCM/LDAP	"FAILED_UCM90_AUTHENTICATION"

Sample Log Snippet

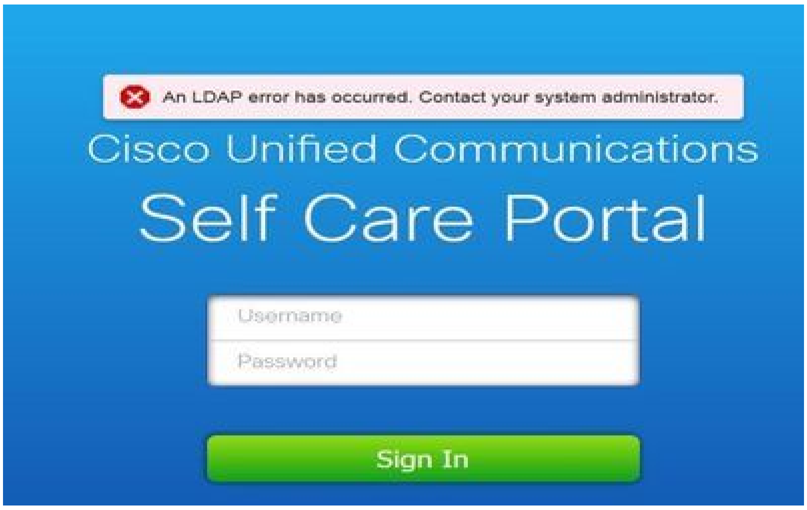
```
<#root>

2017-01-09 08:59:10,652 INFO  [0x00001740] [vices\impl\DiscoveryHandlerImpl.cpp(460)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::ev

FAILED_UCM90_AUTHENTICATION
```

Steps to Resolve

Step 1. Ensure that the User is configured as an **enduser** in CUCM. Navigate to **CUCM Administration > Enduser** page.

Step 2. Verify that credentials are correct and the user is active. Log in to the CUCM Self-care Portal.

This image refers to the scenario where the LDAP is unable to authenticate the user either because the user is not a valid user or the password supplied is incorrect.



An LDAP error has occurred. Contact your system administrator.

Cisco Unified Communications

Self Care Portal

Step 3. If this issue is seen for all users, verify if the LDAP synchronisation and LDAP Authentication settings on **CUCM Administration > System > LDAP** is correct.

> **Tip**: From the LDAP Server perspective, ensure that the **account is not locked,** that the **passwords are not expired,** and that all the **users are synchronized with the CUCM server.**

Error on screen	Cause	What to check in Jabber log
Cannot communicate with the server	Jabber is unable to resolve/reach the CUCM FQDN/HOSTNAME that it received during the Service discovery	"FAILED_UCM90_CONNECTION"

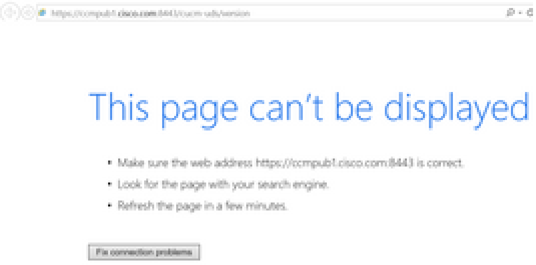
Sample Log Snippet

```
<#root>

2017-08-28 12:04:00,282 INFO  [0x00004290] [vices\impl\DiscoveryHandlerImpl.cpp(452)] [service-discovery] [CSFUnified::DiscoveryHandlerImpl::ev

FAILED_UCM90_CONNECTION
```

Steps to Resolve

Step 1. Test if you are able to open this URL in the browser on the PC https://<CUCM IP/FQDN> :8443/cucm-uds/version

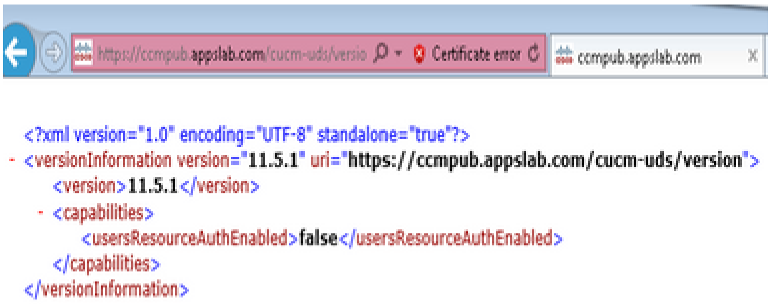
Unsuccessful



This page can’t be displayed

- Make sure the web address https://ccmpub1.cisco.com:8443 is correct.
- Look for the page with your search engine.
- Refresh the page in a few minutes.

Successful



```
  <?xml version="1.0" encoding="UTF-8" standalone="true"?>
- <versionInformation version="11.5.1" uri="https://ccmpub.appslab.com/cucm-uds/version">
      <version>11.5.1</version>
    - <capabilities>
          <usersResourceAuthEnabled>false</usersResourceAuthEnabled>
      </capabilities>
  </versionInformation>
```

Step 2. If the response is unsuccessful, verify that the DNS is configured correctly to resolve them and also if no Network Elements like Firewall/ASA block the port 8443.

Step 3. This URL must be tested for all CUCM Servers in the cluster. For a list of Servers, navigate to **CUCM Administration** > **System** > **Server.**

Error on screen	**Cause**	**What to check in Jabber log**
Cannot communicate with the server	This error is seen when the userid entered in Jabber does not match with the userid configured in CUCM	"FAILED_USER_LOOKUP"

Sample Log Snippet

```
<#root>

2016-08-18 13:14:49,943 INFO  [0x000036e4] [vices\impl\DiscoveryHandlerImpl.cpp(367)] [service-discovery] [DiscoveryHandlerImpl::evaluateService

FAILED_USER_LOOKUP
```

Steps to Resolve

Step 1. Verify that you are able to open this URL in the browser on the PC **https://CUCM:8443/cucm-uds/clusterUser?username=<userid>**

Step 2. Verify that the userid that is entered in Jabber matches the userid on CUCM End-user page.

> **Tip**: Jabber has UPN discovery enabled by default and hence get the **userid** prepopulated from the LDAP UPN field. Check if UPN is the same as configured in CUCM, if you need to disable UPN discovery, **set** UPN_DISCOVERY_ENABLED=false during installation

Stage 3. SOAP Log in (IM and Presence Log in)

Error on screen	**Cause**	**What to check in Jabber log**
Your username or password is not correct	This error is caused due to user Authentication failure	"LERR_CUP_AUTH"

Sample Log Snippet

```
<#root>

2017-01-14 15:55:09,615 INFO  [0x00000dc0] [ts\adapters\imp\components\Login.cpp(99)] [imp.service] [IMPStackCap::Login::OnLoginError] - ******
2017-01-14 15:55:09,615 INFO  [0x00000dc0] [s\adapters\imp\components\Login.cpp(100)] [imp.service] [IMPStackCap::Login::OnLoginError] - OnLog

LERR_CUP_AUTH <12>:


201-01-14 15:55:09,615 INFO  [0x00000dc0] [s\adapters\imp\components\Login.cpp(101)] [imp.service] [IMPS
```

Steps to Resolve

Step 1. Verify that the user is assigned to a Presence node and there are no duplicates for the user (**IM and presence Administration > Diagnostics > System troubleshooter**).

Step 2. Verify that the High Availability (HA) state is Normal and no Failover has occurred.

If you have tried to assign the user during an abnormal HA state, Users are not assigned to any IMP node and log in fails.

Recover the HA state first and re-assign the user.

Step 3. Verify that the credentials are valid.

1. In the case of an LDAP user, verify if the user is able to log in to the CUCM Selfcare portal.

2. If **ccmenduser** page log in fails, check the LDAP Authentication settings in CUCM and also verify the same settings are replicated to IMP

   ```
   run sql select * from ldapauthentication
    run sql select * from ldapauthenticationhost
   ```

3. Verify that the account is not locked in LDAP

4. If the user was recently enabled for Presence, restart the Cisco Sync Agent service on IMP Publisher.

Step 4. Check the server has high TOMCAT CPU consumption

- **show process load**
- **utils diagnose test**

Step 5. Set these services log to DEBUG and then recreate the Log in issue and collect the logs

- Client Profile Agent
- Cisco Tomcat
- Event Viewer-Application Log
- Event Viewer-System Log

Error on screen	**Cause**	**What to check in Jabber log**
Invalid Credentials	This error is caused when the user is not active or in the database.	LERR_CUP_AUTH <10>

Sample Log Snippet

```
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - **************************************
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - OnLog inError: LERR_CUP_AUTH <10>:
[IMPServices] [CSFUnified::IMPStackCap::Log in::OnLog inError] - **************************************
[http-bio-443-exec-15] handlers.Log inHandlerAbstract - preLog in:PRELOGIN reasoncode=FAILURE. User eith
```

Tip: For this error, it is also recommended to retrieve the Cisco Tomcat logs from the CUCM and IM&P servers.

From the Cisco Tomcat logs

<#root>

```
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : inside check wit
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.Certificates - getCNs :
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : cns = [ldap.cisc
2019-10-27 18:33:40,373 DEBUG [http-bio-443-exec-5] impl.Certificates - getDNSSubjectAlts :
2019-10-27 18:33:40,374 DEBUG [http-bio-443-exec-5] impl.LDAPHostnameVerifier - check : subjectAlts = [l

2019-10-27 18:33:40,374 ERROR [http-bio-443-exec-5] impl.AuthenticationLDAP - verifyHostName:Exception.j


2019-10-27 18:33:40,374 DEBUG [http-bio-443-exec-5] impl.AuthenticationLDAP - value of hostnameverifiedf
2019-10-27 18:33:40,374 INFO [http-bio-443-exec-5] impl.AuthenticationLDAP - verifyHostName: Closing LDA
```

Steps to Resolve

Two situations are encountered here if the Cisco Tomcat logs do not show any certificate error, this requires to be validated.

Step 1. Validate that the user is associated with an IM&P server

- Navigate to the **CUCM Administration webpage** > **User Management** >**User Management** > **Assign Presence Users** > Look for the **userid** and **Click** Find

Step 2. If the user is associated with an IM&P server, bounce the user from the Home Node cluster

- Navigate to the **CUCM Administration webpage > User Management > End User > Look** for the **end-user** and click **Find>** under **Service Settings,** uncheck the **Home Cluster** checkbox **>** click **Save>** check the **Home Cluster** checkbox and click **Save**

In case the Cisco Tomcat logs show the error from the Snippet previously showed, perform these steps:

Step 1. Confirm if the Cisco Jabber is configured to use Secure LDAP

Step 2. If Secure LDAP is in use, confirm the certificates' information associated with them like the Fully Qualified Domain Name (FQDN), Hostname and Common Name (CN).

Step 3. Validate how the CUCM and IM&P are configured, if with IP address or FQDN, and compare that with the information contain within the certificate

- Navigate to the **CUCM Administration webpage > System > Server**

Step 4. If the servers are configured with IP address and the LDAP certificates are configured with FQDN, the next command requires to be executed on all the CUCM and IM&P nodes

- **utils ldap config ipaddr**
- Or the definition of the servers requires to be changed as FQDN. Refer to. Change CUCM Server Definition from IP Address or Hostname to FQDN guide.

Error on screen	Cause	What to check in Jabber log
Cannot communicate with the server	This error is caused due to Issues with IMDB or TCP connectivity to IMP	"LERR_CUP_UNREACHABLE" , "LERR_CUP_TIMEOUT"

Sample Log Snippet

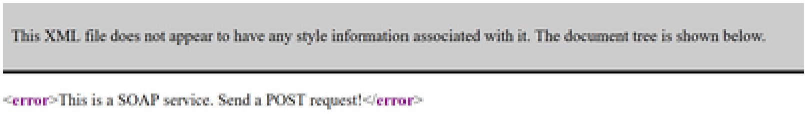
```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
2017-11-08 16:03:20,051 INFO  [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLogin
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
```

Steps to Resolve

Step 1. Verify that IMP FQDN/Hostnames are resolvable from the client PC.

Step 2. Verify that you can open this URL in browser **https://<IMP SERVER FQDN/IP>:8443/EPASSoap/service/v105**

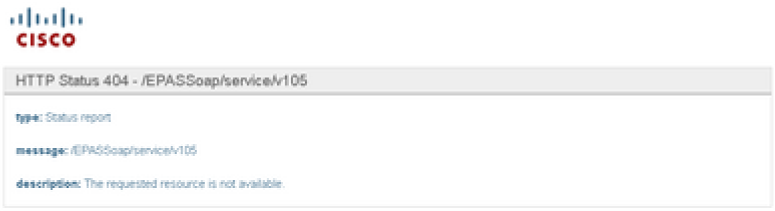
Successful



This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
<error>This is a SOAP service. Send a POST request!</error>
```

Unsuccessful



HTTP Status 404 - /EPASSoap/service/v105

type: Status report

message: /EPASSoap/service/v105

description: The requested resource is not available.

Step 3. Verify that firewall/VPN does not block the connectivity to IMP server (Port 8443,5222)

Step 4. Verify if this service runs in IMP server: Cisco Client profile Agent

Step 5. Set these services log to DEBUG, recreate the Log in issue and then collect the logs if the previous steps do not resolve the problem.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent

> **Tip**: If the problem persists for only one user, un-assign and re-assign the user for presence in CUCM. If it is a system-wide problem, collect the logs and check the status of the services

---

Error on screen	**Cause**	**What to check in Jabber log**
Cannot communicate with the server	Usually, this error is caused due to Issues with IMDB	"LERR_CUP_INTERNAL_ERROR"

Sample Log Snippet

```
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(127)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
2017-11-08 16:03:20,051 INFO  [0x00003a0c] [s\adapters\imp\components\Login.cpp(128)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLogin
2017-11-08 16:03:20,051 DEBUG [0x00003a0c] [s\adapters\imp\components\Login.cpp(129)] [IMPServices] [CSFUnified::IMPStackCap::Login::OnLog
```

Steps to Resolve

Step 1. Perform Mandatory checks

Step 2. Verify that these services are running in the IM&P server

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

- Cisco Log in datastore

Step 3. Check if this Field notice is applicable

Field Notice: FN - 64267 - Cisco Unified Communications Manager IM & Presence causes Cisco Jabber log in failures - Software Upgrade Recommended

Step 4. Set these services log to DEBUG, recreate the Log in issue and then collect the logs if the previous steps do not resolve the problem.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Cisco Log in Datastore
- Event Viewer-Application Log
- Event Viewer-System Log

Step 5. Reboot the cluster to recover the situation.

Stage 4. XMPP Log in (IM and Presence Log in)

Error on screen	Cause	What to check in Jabber log
Cannot communicate with the server	Commonly seen when Jabber fails to connect over MRA and cannot establish a TLS session with the IM&P	LERR_JABBER_AUTH <14>: Authentication error with server, for example resource bind, TLS, create session or SASL error

Sample Log Snippet

```
2019-05-03 15:19:32,225 DEBUG [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(128)] [IMPServi
2019-05-03 15:19:32,225 INFO  [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(129)] [IMPServi
2019-05-03 15:19:32,225 DEBUG [0x0000000109732f80] [s/adapters/imp/components/Log in.cpp(130)] [IMPServi
```

Steps to Resolve

Step 1. Verify that port 5222 is opened between the IM&P servers and the Expressways.

Step 2. Verify that these services are running in the IM&P server and restart them once.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

Step 3. Disable the High Availability from the CUCM Presence Redundancy Groups.

Step 4. Restart the **Cisco XCP Router service** on all the IM&P nodes, first with the IM&P Publisher and then in the Subscribers.

- **utils service restart Cisco XCP Router Service**

Step 5. Reenable the High Availability from the CUCM Presence Redundancy Groups.

Error on screen	**Cause**	**What to check in Jabber log**
Cannot communicate with the server	Commonly seen when Jabber cannot create a session and bind itself in IMP server	LERR_JABBER_AUTH <17>: Authentication error with server, for example resource bind, TLS, create session or SASL error"

Sample Log Snippet

```
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(127)] [IMPServices] [OnLoginError] - **************
2017-10-27 10:56:47,396 INFO  [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(128)] [IMPServices] [OnLoginError] - OnLoginError: LE
2017-10-27 10:56:47,396 DEBUG [0x00007fff8b3d7340] [s/adapters/imp/components/Login.cpp(129)] [IMPServices] [OnLoginError] - **************
```

Steps to Resolve

Step 1. Verify that the cup-xmpp Certificates are valid.

Step 2. Verify that Port 5222 is open.

Step 3. Set these services log to DEBUG and then recreate the Log in issue and collect the logs before step 4.

If Root cause to be identified as Reboot of the server is the only fix known.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Application Log
- Event Viewer-System Log

Step 4. Reboot the server to resolve the issue.

Error on screen	**Cause**	What to check in Jabber log
Cannot communicate with the server	Seen when IMP is not resolvable or reachable due to Network problems like firewall	"LERR_JABBER_UNREACHABLE "

Sample Log Snippet

```
2014-12-15 12:07:31,600 INFO  [0x00001670] [ts\adapters\imp\components\Login.cpp(96)] [imp.service] [IMPStackCap::Login::OnLoginError] - ******
2014-12-15 12:07:31,600 INFO  [0x00001670] [ts\adapters\imp\components\Login.cpp(97)] [imp.service] [IMPStackCap::Login::OnLoginError] - OnLog
2014-12-15 12:07:31,600 INFO  [0x00001670] [ts\adapters\imp\components\Login.cpp(98)] [imp.service] [IMPStackCap::Login::OnLoginError] - ******
```

Steps to Resolve

Step 1. Check if IMP FQDN/Hostnames are resolvable.

Step 2. Verify that the firewall/VPN does not block the connectivity to the IM&P server (Port 8443,5222).

Step 3. Verify if these services are running in the IM&P server and restart them once.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service

Step 4. Perform Mandatory checks.

Step 5. Set these services log to DEBUG, recreate the Log in issue and then collect the logs if the previous steps do not resolve the problem.

- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Application Log
- Event Viewer-System Log

Step 6. In case of all users experience the same error, a server Reboot can be done for quick recovery.

Error on screen	**Cause**	What to check in Jabber log
Cannot Sign in your account. Contact your administrator.	Commonly seen when the Jabber is log in with SSO, either on-prem or over Expressways (Mobile Remote Access (MRA))	"Log inErrortoErrorCode: 27 mapped to: UnknownLog inError "

Sample Log Snippet

```
2020-03-12 19:55:01,283 DEBUG [0x000000010b71d800][apters/imp/components/Log inUtils.cpp(96)][IMPService
2020-03-12 19:55:01,283 DEBUG [0x000000010b71d800][isteners/Log inEventListenerImpl.cpp(148)][IMPService
2020-03-12 19:55:01,283 INFO [0x000000016b61f000][ers/imp/lifecycle/Log inExecutor.cpp(314)][IMPServices
2020-03-12 19:55:01,478 INFO [0x000000010b71d800][pp/tahiti/ui/log in/YLCLog inBaseVC.m(500)][UI.Action.
```

Steps to Resolve

Step 1. Validate that the user is assigned to the IM&P.

Step 2. Validate that the certificates are correctly exchanged between the nodes and the Jabber.

Step 3. Validate the OAuth Signing and Encryption keys are correctly configured on all the nodes. See this document under Verify section.

Step 4. Perform Mandatory checks.

Step 5. Set these services log to DEBUG, recreate the Log in issue and then collect the logs if the previous steps do not resolve the problem.

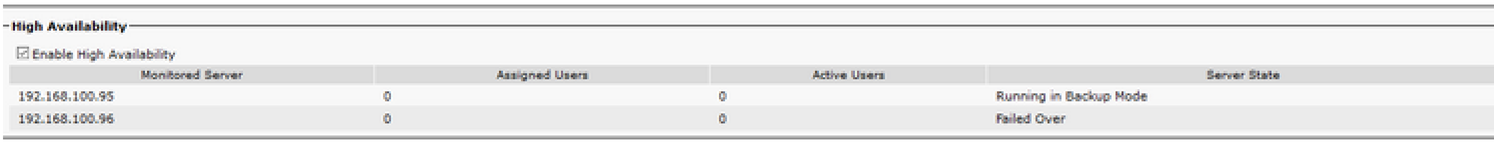
- Cisco XCP Router
- Cisco XCP Connection Manager
- Cisco XCP Authentication Service
- Client Profile Agent
- Event Viewer-Application Log
- Event Viewer-System Log
- Cisco SSO
- Cisco Tomcat
- Cisco Tomcat Security

Mandatory Checks

Step 1. Verify that the user is assigned to a Presence node (navigate to **IM and Presence Administration** > **System** > **Topology)** and there are no duplicates for the user (navigate to **IM and Presence Administration** > **Diagnostics** > **System troubleshooter)**

Step 2. If High Availability is enabled, navigate to **CUCM Administration** > **Server** > **Presence Redundancy Group** and check if they are in **Normal state**. This is the image of how Normal state looks. For more information about High Availability can be found here.

Abnormal State



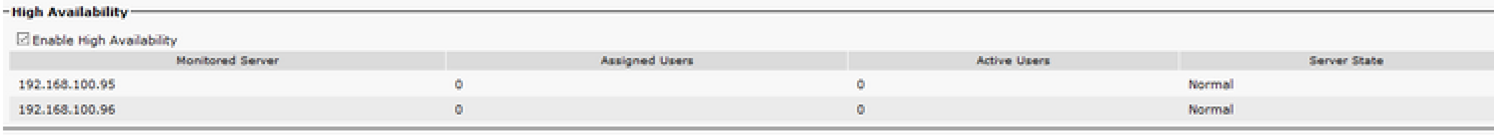
High Availability

☑ Enable High Availability

Monitored Server	Assigned Users	Active Users	Server State
192.168.100.95	0	0	Running in Backup Mode
192.168.100.96	0	0	Failed Over

> **Note**: These services are used by the Jabber to log in: Cisco Tomcat, Cisco Tomcat Security, Cisco Client Profile Agent, Cisco XCP Connection Manager, Cisco XCP Router and Cisco XCP Authentication.

Normal State



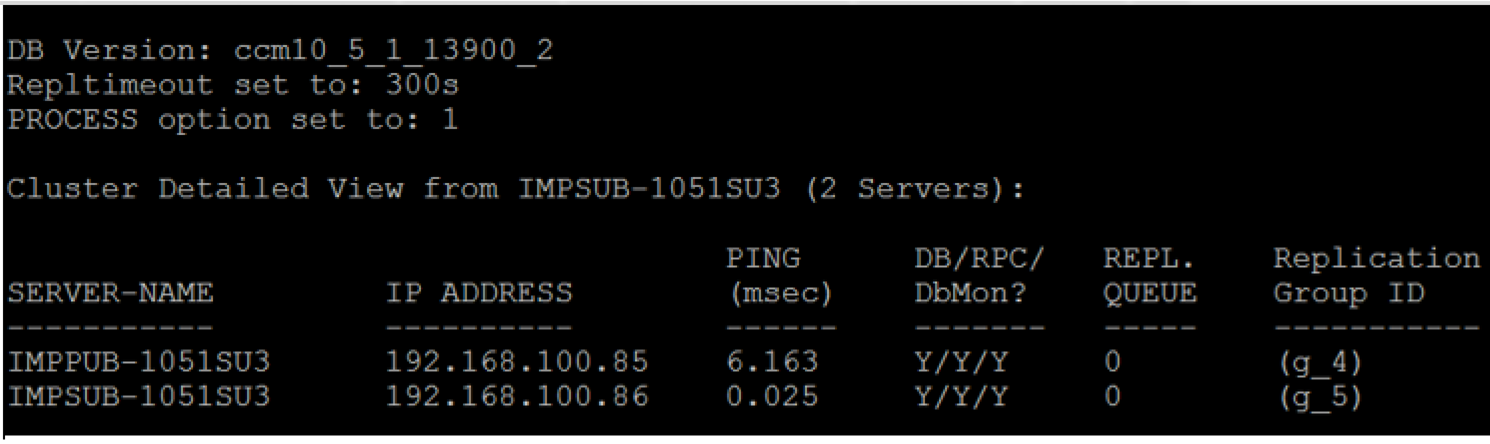
High Availability

☑ Enable High Availability

Monitored Server	Assigned Users	Active Users	Server State
192.168.100.95	0	0	Normal
192.168.100.96	0	0	Normal

Step 3. Check High Availability Replication status.

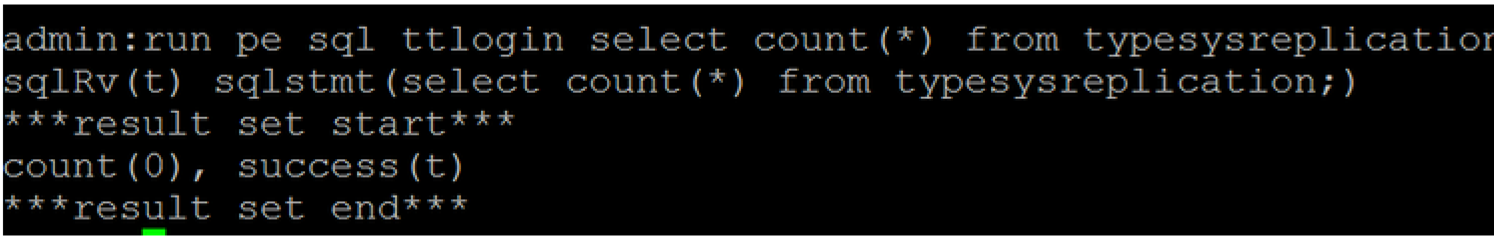
a.utils dbreplication runtimestate



```
DB Version: ccm10_5_1_13900_2
Repltimeout set to: 300s
PROCESS option set to: 1

Cluster Detailed View from IMPSUB-1051SU3 (2 Servers):

                                    PING      DB/RPC/   REPL.    Replication
SERVER-NAME         IP ADDRESS      (msec)    DbMon?    QUEUE    Group ID
-----------         ----------      ------    -------   -----    -----------
IMPPUB-1051SU3      192.168.100.85  6.163     Y/Y/Y     0        (g_4)
IMPSUB-1051SU3      192.168.100.86  0.025     Y/Y/Y     0        (g_5)
```

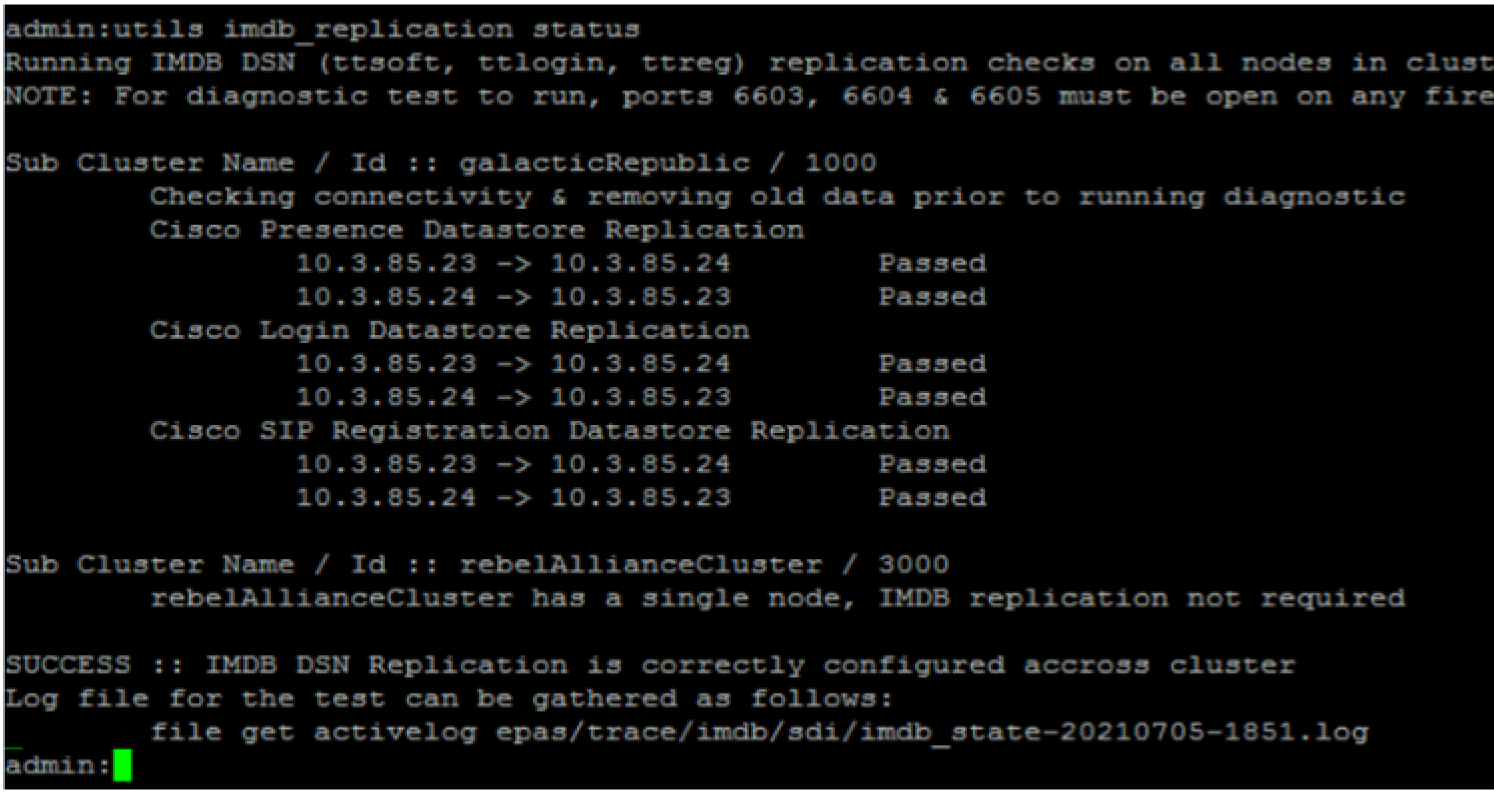
If you encounter issues on the database replication, [navigate to this link.](#)

b.run pe sql ttlog in select count(*) from typesysreplication



```
admin:run pe sql ttlogin select count(*) from typesysreplicatio
sqlRv(t) sqlstmt(select count(*) from typesysreplication;)
***result set start***
count(0), success(t)
***result set end***
```

or utils imdb_replication status (10.5.2 SU2a and later)



```
admin:utils imdb_replication status
Running IMDB DSN (ttsoft, ttlogin, ttreg) replication checks on all nodes in clust
NOTE: For diagnostic test to run, ports 6603, 6604 & 6605 must be open on any fire

Sub Cluster Name / Id :: galacticRepublic / 1000
        Checking connectivity & removing old data prior to running diagnostic
        Cisco Presence Datastore Replication
                10.3.85.23 -> 10.3.85.24        Passed
                10.3.85.24 -> 10.3.85.23        Passed
        Cisco Login Datastore Replication
                10.3.85.23 -> 10.3.85.24        Passed
                10.3.85.24 -> 10.3.85.23        Passed
        Cisco SIP Registration Datastore Replication
                10.3.85.23 -> 10.3.85.24        Passed
                10.3.85.24 -> 10.3.85.23        Passed

Sub Cluster Name / Id :: rebelAllianceCluster / 3000
        rebelAllianceCluster has a single node, IMDB replication not required

SUCCESS :: IMDB DSN Replication is correctly configured accross cluster
Log file for the test can be gathered as follows:
        file get activelog epas/trace/imdb/sdi/imdb_state-20210705-1851.log
admin:
```

The three datastores need to show **PASSED,** and the command needs to be run on all the IM&P nodes, as sometimes on one node all the datastores' replication can show **Passed**, but on another node, it can show **Failed.**

The implications if the IMDB (In-memory Database) replication is not correct can imply that some or all the users are unable to log in or that their presence status cannot be shown correctly.

The steps to resolve the IMDB replication issues are:

Step 1. Disable the High Availability (HA) for the IM&P Subcluster that is affected.

Step 2. Stop the Cisco Presence Engine on all nodes

utils service stop *Cisco Presence Engine*

Step 3. Verify all the Datastore Services are running: Cisco Log in Datastore, Cisco Route Datastore, Cisco Presence Datastore, Cisco SIP Registration Datastore.

utils service list

Step 4. Restart Cisco Config Agent on each node one at a time.

utils service restart Cisco Config Agent

Step 5. Start Cisco Presence Engine.

utils service start Cisco Presence Engine

Step 6. Enable HA for the Sub-cluster.

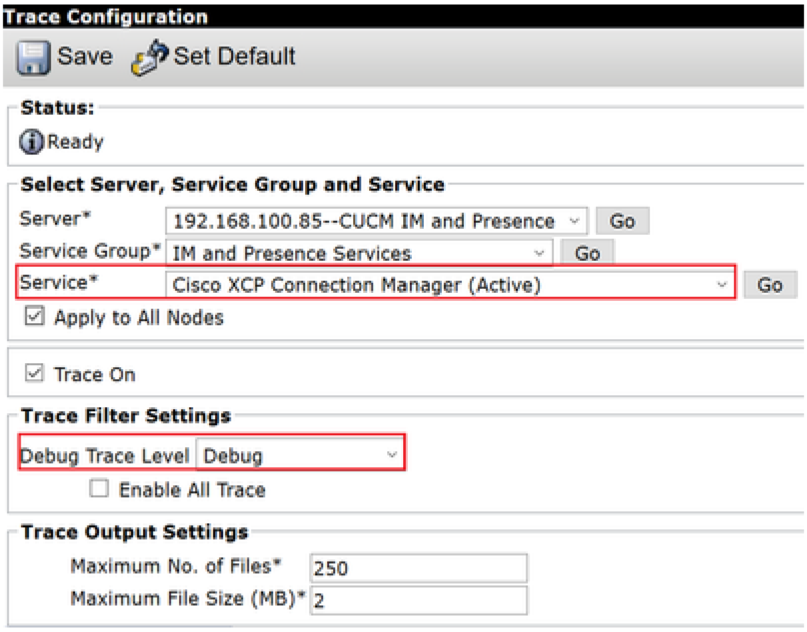
How to Set Logs to DEBUG

Step 1 Choose **Navigation** > **Unified serviceability** > **Trace** > **Configuration**.
Step 2 From the Server drop-down list, choose the server (i.e IMP node) that runs the service to configure trace and click **Go**.
Step 3 From the Service Group drop-down list box, choose the service group for the service to configure trace; then click **Go**.
Step 4 From the Service drop-down list box, choose the service for which you want to configure trace; then click **Go**.
Step 5 Check box '**Apply to All Nodes**' and select the trace level to '**DEBUG**'
Step 6 To save your trace parameters configuration, click the **Save** button

For more information on how to set trace levels refer to the Cisco Unified Serviceability Administration Guide.

Helpful videos:

- Collect logs from the RTMT



Trace Configuration

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence

Service Group* IM and Presence Services

Service* Cisco XCP Connection Manager (Active)

☑ Apply to All Nodes

☑ Trace On

Trace Filter Settings

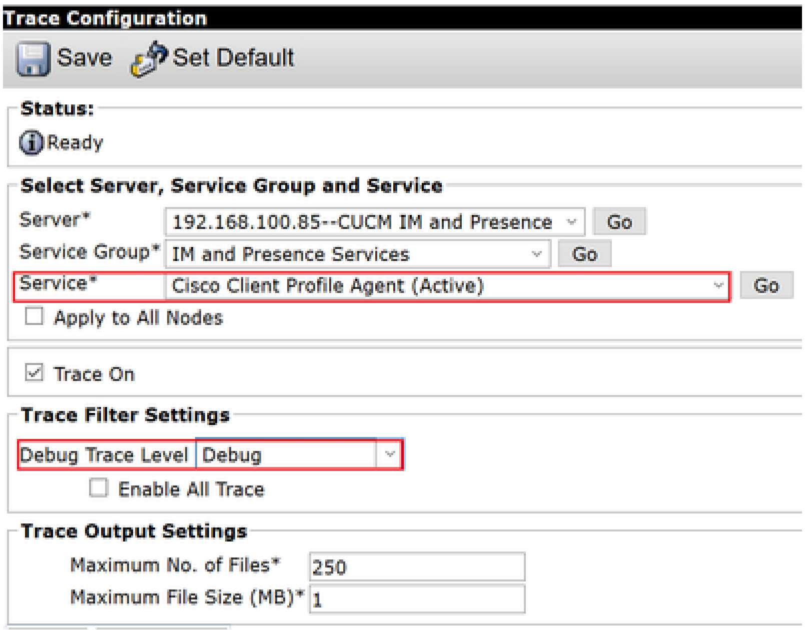
Debug Trace Level Debug

☐ Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 2



Trace Configuration

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence

Service Group* IM and Presence Services

Service* Cisco Client Profile Agent (Active)

☐ Apply to All Nodes

☑ Trace On

Trace Filter Settings

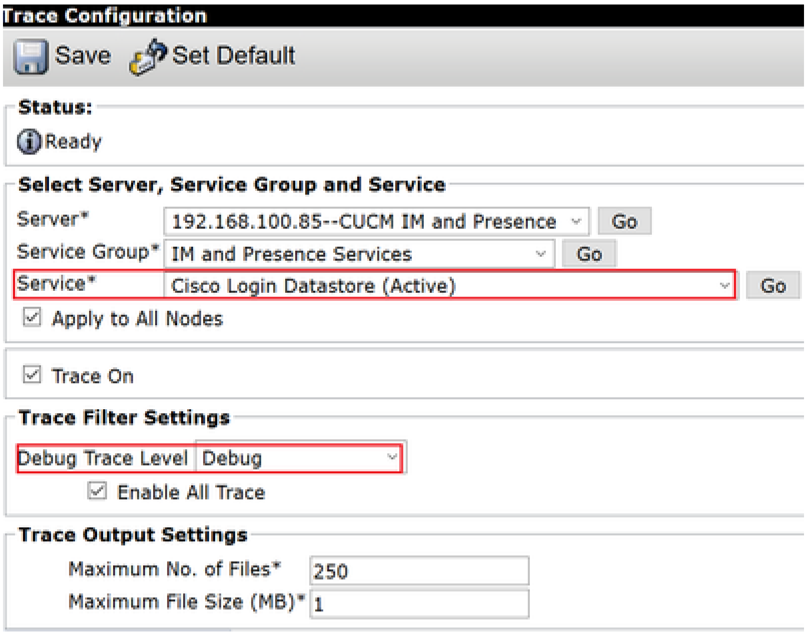
Debug Trace Level Debug

☐ Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 1



Trace Configuration

Status:
Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence

Service Group* IM and Presence Services

Service* Cisco Login Datastore (Active)

☑ Apply to All Nodes

☑ Trace On

Trace Filter Settings

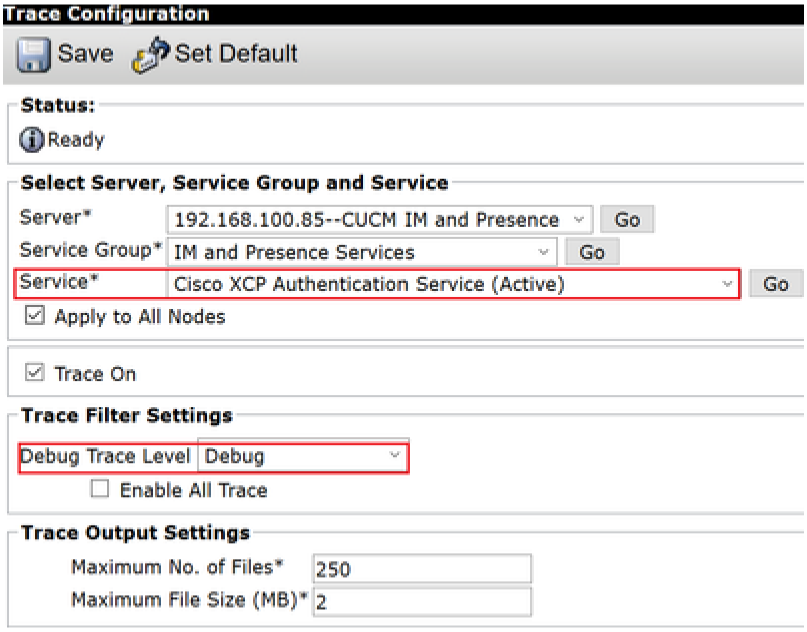
Debug Trace Level Debug

☑ Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 1



Trace Configuration

Save | Set Default

Status:

Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence | Go

Service Group* IM and Presence Services | Go

Service* Cisco XCP Authentication Service (Active) | Go

☑ Apply to All Nodes

☑ Trace On

Trace Filter Settings

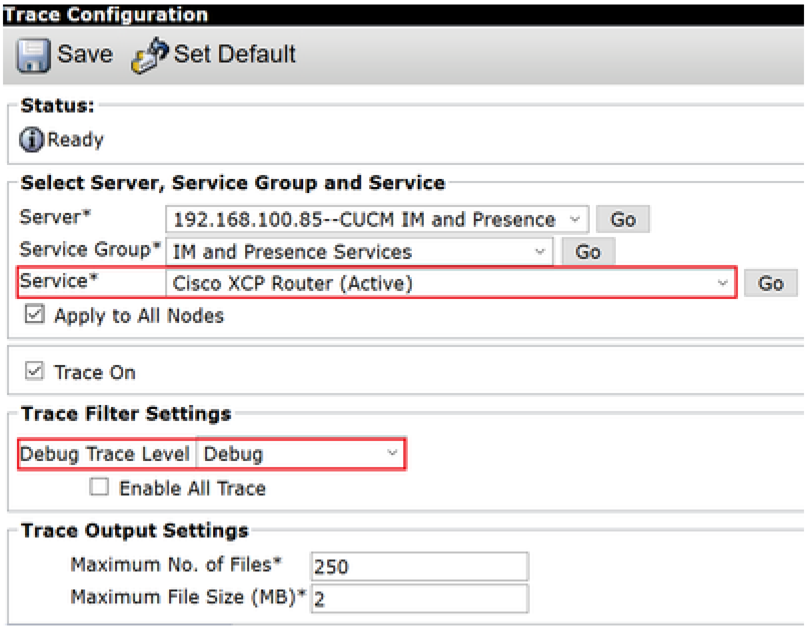
Debug Trace Level Debug

☐ Enable All Trace

Trace Output Settings

Maximum No. of Files* 250

Maximum File Size (MB)* 2



Trace Configuration

Save | Set Default

Status:

Ready

Select Server, Service Group and Service

Server* 192.168.100.85--CUCM IM and Presence | Go

Service Group* IM and Presence Services | Go

Service* Cisco XCP Router (Active) | Go

☑ Apply to All Nodes

☑ Trace On

Trace Filter Settings

Debug Trace Level Debug

☐ Enable All Trace

Trace Output Settings

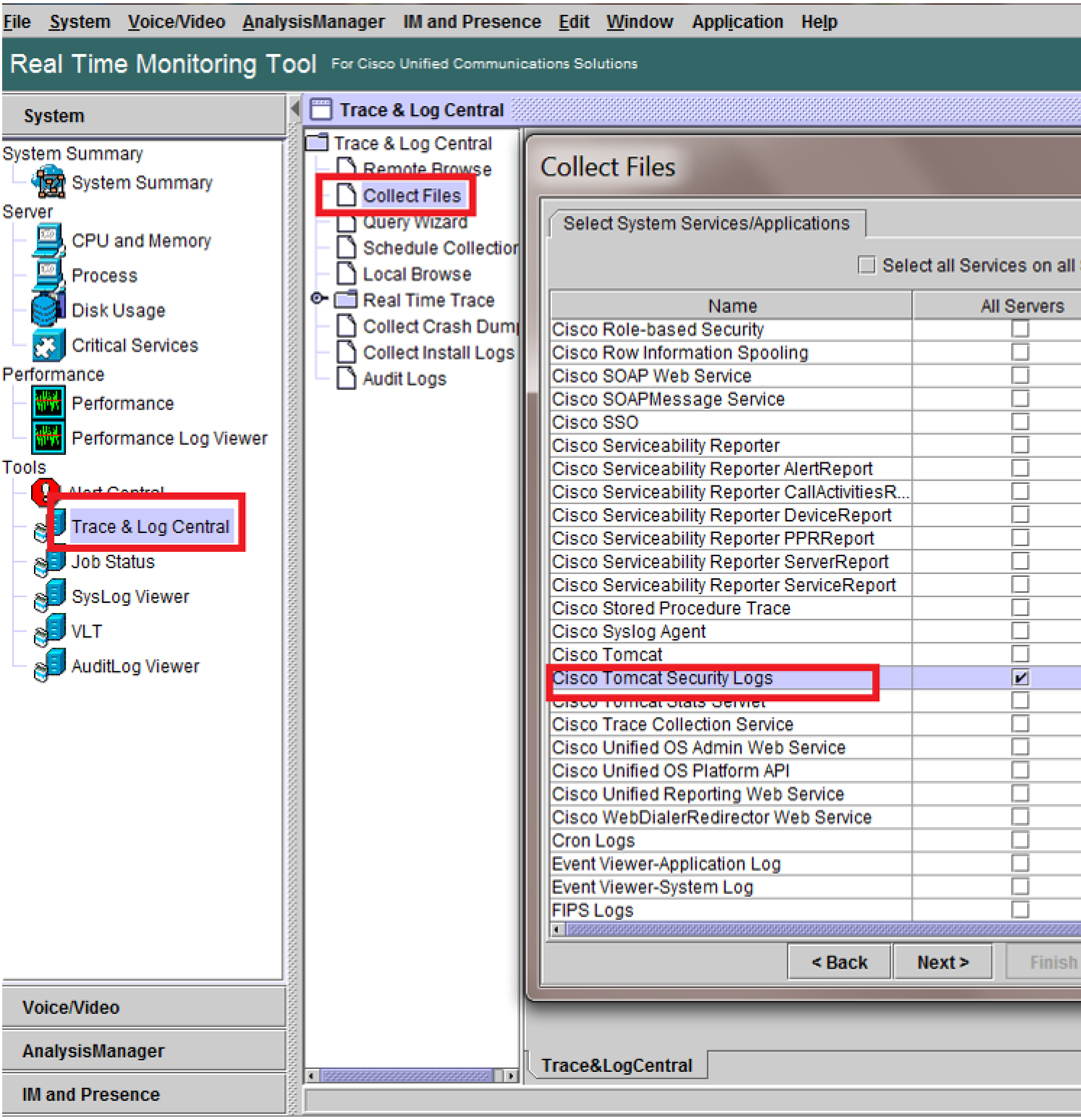
Maximum No. of Files* 250

Maximum File Size (MB)* 2

Logs to Collect

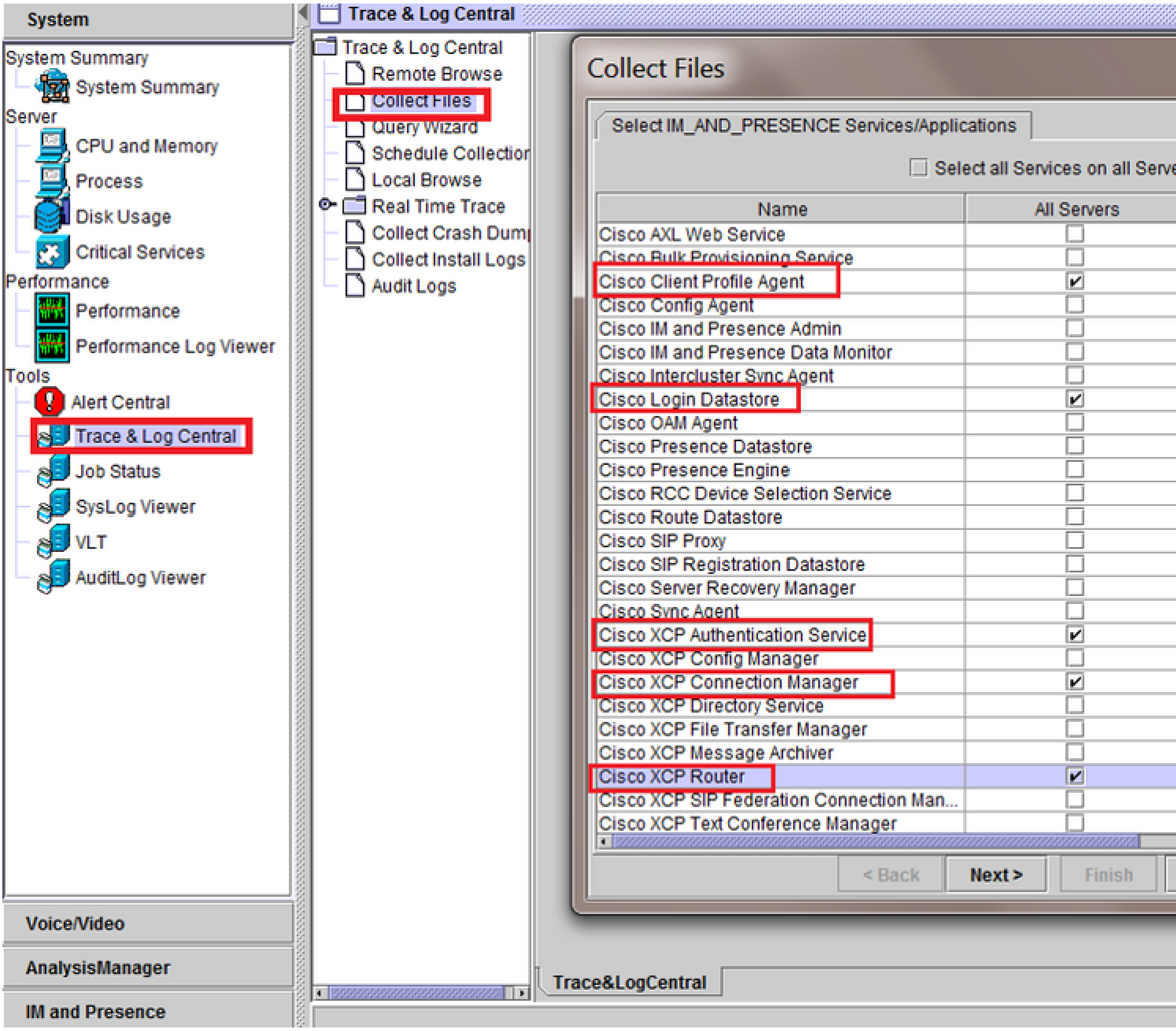
RTMT	Admin CLI
Cisco Client Profile Agent	**file get activelog tomcat/logs/epassoap/log4j/***
Cisco Log in Datastore	**file get activelog epas/trace/imdb/sdi/ttlog in/**
Cisco Tomcat Security Logs	**file get activelog tomcat/logs/security/log4j/***
Cisco XCP Authentication Service	**file get activelog epas/trace/xcp/log/auth***
Cisco XCP Connection Manager	**file get activelog epas/trace/xcp/log/client-cm-1*.log**
Cisco XCP Router	**file get activelog epas/trace/xcp/log/rtr-jsm-1**
Event Viewer-Application Log	**file get activelog syslog/CiscoSyslog***
Event Viewer-System Log	**file get activelog syslog/messages***

Collect Logs from RTMT



□ Select all Services on all

Name	All Servers
Cisco Role-based Security	□
Cisco Row Information Spooling	□
Cisco SOAP Web Service	□
Cisco SOAPMessage Service	□
Cisco SSO	□
Cisco Serviceability Reporter	□
Cisco Serviceability Reporter AlertReport	□
Cisco Serviceability Reporter CallActivitiesR...	□
Cisco Serviceability Reporter DeviceReport	□
Cisco Serviceability Reporter PPRReport	□
Cisco Serviceability Reporter ServerReport	□
Cisco Serviceability Reporter ServiceReport	□
Cisco Stored Procedure Trace	□
Cisco Syslog Agent	□
Cisco Tomcat	□
Cisco Tomcat Security Logs	☑
Cisco Tomcat Stats Servlet	□
Cisco Trace Collection Service	□
Cisco Unified OS Admin Web Service	□
Cisco Unified OS Platform API	□
Cisco Unified Reporting Web Service	□
Cisco WebDialerRedirector Web Service	□
Cron Logs	□
Event Viewer-Application Log	□
Event Viewer-System Log	□
FIPS Logs	□



Collect Files

Select IM_AND_PRESENCE Services/Applications

□ Select all Services on all Serve

Name	All Servers
Cisco AXL Web Service	□
Cisco Bulk Provisioning Service	□
Cisco Client Profile Agent	☑
Cisco Config Agent	□
Cisco IM and Presence Admin	□
Cisco IM and Presence Data Monitor	□
Cisco Intercluster Sync Agent	□
Cisco Login Datastore	☑
Cisco OAM Agent	□
Cisco Presence Datastore	□
Cisco Presence Engine	□
Cisco RCC Device Selection Service	□
Cisco Route Datastore	□
Cisco SIP Proxy	□
Cisco SIP Registration Datastore	□
Cisco Server Recovery Manager	□
Cisco Sync Agent	□
Cisco XCP Authentication Service	☑
Cisco XCP Config Manager	□
Cisco XCP Connection Manager	☑
Cisco XCP Directory Service	□
Cisco XCP File Transfer Manager	□
Cisco XCP Message Archiver	□
Cisco XCP Router	☑
Cisco XCP SIP Federation Connection Man...	□
Cisco XCP Text Conference Manager	□