

Troubleshoot IM&P Services Displayed as "Unknown" in the Presence Topology

Contents

[Introduction](#)

[Background Information](#)

[Problem](#)

[Solution](#)

[Required Logs](#)

[What to Expect in the Logs](#)

Introduction

This document describes how to troubleshoot the Presence Topology page when it shows the services as Unknown on the Instant Message and Presence (IM&P) server nodes.




















Background Information

When you navigate to the **IM&P Administration web page > System > Presence Topology** to verify the health status of the server, you might encounter that the server is not in its correct state. In this case, the server shows a white cross within a red circle, even though the services are started as shown on the Command Line Interface (CLI) via the **utils service list** command.

This document describes the most common reasons these errors are displayed on the Presence Topology webpage and how to fix them.

Problem

When you choose **view** on one of the affected nodes, you can see these errors on the webpage: the status of the services are **unknown**:

Node Detail	
Test	
Verify IM/P Service Installed	 IM/P Service is Installed
Verify Node Reachable (pingable)	 Node is Reachable
Version	 11.5.1.15900(33)
Service Name	Status
Cisco SIP Proxy	 UNKNOWN
Cisco Presence Engine	 UNKNOWN
Cisco Login Datastore	 UNKNOWN
Cisco Presence Datastore	 UNKNOWN
Cisco Route Datastore	 UNKNOWN
Cisco SIP Registration Datastore	 UNKNOWN
A Cisco DB	 UNKNOWN
Cisco XCP Router	 UNKNOWN
Cisco XCP Connection Manager	 UNKNOWN
Cisco XCP Authentication	 UNKNOWN
Cisco XCP SIP Federation Connection Manager	 UNKNOWN
Cisco XCP Message Archiver	 UNKNOWN
Cisco Client Profile Agent	 UNKNOWN
Cisco Sync Agent	 UNKNOWN
Cisco Inter-Cluster Sync Agent	 UNKNOWN
Cisco XCP Text Conference Manager	 UNKNOWN

However, if you access the CLI Secure Shell (SSH) session of the IM&P Server and run the command: **utils service list**, you see that all those services are actually in the "STARTED" state.

```

>> Return code = 0
A Cisco DB{STARTED}
A Cisco DB Replicator{STARTED}
Cisco AMC Service{STARTED}
Cisco AXL Web Service{STARTED}
Cisco Audit Event Service{STARTED}
Cisco Bulk Provisioning Service{STARTED}
Cisco CDP{STARTED}
Cisco CDP Agent{STARTED}
Cisco CallManager Serviceability{STARTED}
Cisco CallManager Serviceability RTMT{STARTED}
Cisco Certificate Expiry Monitor{STARTED}
Cisco Client Profile Agent{STARTED}
Cisco Config Agent{STARTED}
Cisco DRF Local{STARTED}
Cisco Database Layer Monitor{STARTED}
Cisco IM and Presence Admin{STARTED}
Cisco IM and Presence Data Monitor{STARTED}
Cisco Intercluster Sync Agent{STARTED}
Cisco Log Partition Monitoring Tool{STARTED}
Cisco Login Datastore{STARTED}
Cisco Management Agent Service{STARTED}
Cisco OAM Agent{STARTED}
Cisco Presence Datastore{STARTED}
Cisco Presence Engine{STARTED}
Cisco RCC Device Selection Service{STARTED}
Cisco RIS Data Collector{STARTED}
Cisco RTMT Reporter Servlet{STARTED}
Cisco Route Datastore{STARTED}
Cisco SIP Proxy{STARTED}
Cisco SIP Registration Datastore{STARTED}
Cisco Server Recovery Manager{STARTED}
Cisco Sync Agent{STARTED}
Cisco Syslog Agent{STARTED}
Cisco Tomcat{STARTED}
Cisco Tomcat Stats Servlet{STARTED}
Cisco Trace Collection Service{STARTED}
Cisco Trace Collection Servlet{STARTED}
Cisco XCP Authentication Service{STARTED}
Cisco XCP Config Manager{STARTED}
Cisco XCP Connection Manager{STARTED}
Cisco XCP Message Archiver{STARTED}
Cisco XCP Router{STARTED}

```

Solution

The error on the GUI is associated with a Tomcat certificate issue. Here is what is required to be verified:

Step 1. Make sure that all your **Tomcat** and **Tomcat-trust** certificates are not expired, otherwise, those need to be regenerated.

Step 2. If your server uses CA-Signed certificates, you need to validate that the whole Tomcat chain is complete. This means that the intermediates and Root certificates are required to be uploaded as Tomcat-trust.

Here is an example of a missing certificate in the Tomcat chain. In this case, the Tomcat certificate chain consists of only two certificates: Root > Leaf, however, there are scenarios where more than 2 or 3 intermediate certificates build the chain.

Certificate	Common Name	Type	Key Type	Distribution	Issued By	Expiration	Description
tomcat	tenochtitlanCM.ms.mexrus.ru	CA-signed	RSA	Multi-server(SAN)	mexrus-TENOCHTITLAN-CA	12/13/2021	Certificate Signed by mexrus-TENOCHTITLAN-CA
tomcat-ECDSA	tenochtitlanIMP-EC.mexrus.ru	Self-signed	EC	tenochtitlanIMP.mexrus.ru	tenochtitlanIMP-EC.mexrus.ru	12/10/2024	Self-signed certificate generated by system
tomcat-trust	tenochtitlanIMP-EC.mexrus.ru	Self-signed	EC	tenochtitlanIMP.mexrus.ru	tenochtitlanIMP-EC.mexrus.ru	12/10/2024	Trusted local cluster own-certificate
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3	CA-signed	RSA	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/07/2020	Cert imported from CUCM node tenochtitlanCM.mexrus.ru
tomcat-trust	tenochtitlanCM-EC.mexrus.ru	Self-signed	EC	tenochtitlanCM.mexrus.ru	tenochtitlanCM-EC.mexrus.ru	12/08/2024	Cert imported from CUCM node tenochtitlanCM.mexrus.ru
tomcat-trust	tenochtitlanIMP.mexrus.ru	Self-signed	RSA	tenochtitlanIMP.mexrus.ru	tenochtitlanIMP.mexrus.ru	12/10/2024	Trusted local cluster own-certificate

In the image example, the Issuer: **mexrus-TENOCHTITLAN-CA** is the certificate missing.

Required Logs

Navigate to **IM and Presence Serviceability > Trace > Trace Configuration > Server** to select: **IM&P Publisher > Service Group > Database and Admin Services > Service: Cisco IM and Presence Admin > Apply to all Nodes > Debug level: Debug > Check the Enable All Trace Checkbox > Save.**

Navigate to **IM and Presence Administration > System > Presence Topology > Choose the node that is affected by the unknown services, and note the timestamp.**

Open the Cisco Real-Time Monitor Tool (RTMT) and gather these logs:

- Cisco Syslog
- Cisco Tomcat
- Cisco Tomcat Security
- Event Viewer Application Logs
- Event Viewer System Logs
- Cisco IM and Presence Admin logs

What to Expect in the Logs

From the cupadmin*.log

When you access the **Presence Topology > Node panel.**

```
2021-01-23 17:54:57,036 DEBUG [Thread-137] logging.IMPCommonLogger - IMPConnectionFactory: Create socket called with host tenochtitlanIMP.mexrus.ru and port 8443
2021-01-23 17:54:57,040 DEBUG [Thread-137] logging.IMPCommonLogger - Enabled protocols: [TLSv1.1, TLSv1, TLSv1.2]
```

An exception was received because a certificate was not verified.

```
2021-01-23 17:54:57,087 ERROR [Thread-137] services.ServiceUtil - Got an exception setting up the HTTPS connection.
javax.net.ssl.SSLException: Certificate not verified.
at com.rsa.sslj.x.aH.b(Unknown Source)
at com.rsa.sslj.x.aH.a(Unknown Source)
at com.rsa.sslj.x.aH.a(Unknown Source)
at com.rsa.sslj.x.ap.c(Unknown Source)
at com.rsa.sslj.x.ap.a(Unknown Source)
at com.rsa.sslj.x.ap.j(Unknown Source)
at com.rsa.sslj.x.ap.i(Unknown Source)
at com.rsa.sslj.x.ap.h(Unknown Source)
at com.rsa.sslj.x.aS.startHandshake(Unknown Source)
at com.cisco.cup.services.ServiceUtil.init(ServiceUtil.java:118)
at com.cisco.cup.services.ServiceUtil.getServiceInfo(ServiceUtil.java:197)
at com.cisco.cup.services.ServiceUtil.getServiceInfo(ServiceUtil.java:182)
```

When you attempt to retrieve the Node Status for the topology:

at

```
com.cisco.cup.admin.actions.TopologyNodeStatusAction$ServiceRunner.run(TopologyNodeStatusAction.
java:358)
at java.lang.Thread.run(Thread.java:748)
Caused by: com.rsa.sslj.x.aK: Certificate not verified.
at com.rsa.sslj.x.bg.a(Unknown Source)
at com.rsa.sslj.x.bg.a(Unknown Source)
at com.rsa.sslj.x.bg.a(Unknown Source)
... 13 more
```

An exception is caused due to the missing issuer of the Tomcat Certificate.

```
Caused by: java.security.cert.CertificateException: Issuer for signed certificate
[CN=tenochtitlanCM-ms.mexrus.ru,OU=Collab,O=Cisco,L=Mexico,ST=Mexico City,C=MX] not found:
CN=mexrus-TENOCHTITLAN-CA,DC=mexrus,DC=ru
at com.cisco.cup.security.TLSTrustManager.checkServerTrusted(TLSTrustManager.java:309)
at com.rsa.sslj.x.aE.a(Unknown Source)
... 16 more
```

```
2021-01-23 17:54:57,087 DEBUG [Thread-137] actions.TopologyNodeStatusAction$ServiceRunner -
Retrieved service status for node tenochtitlanIMP.mexrus.ru
2021-01-23 17:54:57,088 DEBUG [http-bio-443-exec-8] actions.TopologyNodeStatusAction -
[Topology] VerifyNodeServices - Complete.
```

Another type of exception can be found on the cupadmin*.log traces, which display the error "Incorrect issuer for server cert":

```
Caused by: java.security.cert.CertificateException: Incorrect issuer for server cert
at
com.cisco.cup.security.TLSTrustManager.checkServerTrusted(TLSTrustManager.java:226)
at com.rsa.sslj.x.aE.a(Unknown Source)
... 16 more
```

```
2017-10-14 09:04:01,667 ERROR [Thread-125] services.ServiceUtil - Failed to retrieve service
status. Reason: Certificate not verified.
javax.net.ssl.SSLException: Certificate not verified.
```

In this case, the IM&P does not recognize the Issuer certificate for the Tomcat as a valid Issuer certificate, which most probably was caused due to a corrupted certificate. The **options here are:**

- Validate the information presented on both: Tomcat and Issuer certificates.
- Get another issuer certificate and compare it with the one that is already on the IM&P Trust Store.
- Delete the issuer certificate from the IM&P and upload it again.
- Regenerate the Tomcat CA- Certificate.

Note: Be aware of the Cisco bug Id [CSCvu78005](#), which refers to the Tomcat RSA/ECDSA Keystore's does not update in all nodes when the existed CA certificate in the chain is replaced.

Step 1. Run the **utils diagnose test** command on the affected node.

Step 2. Contact Cisco Technical Assistance Center (TAC) for further assistance.