Configure Multiple Device Messaging

Multiple Device Messaging Overview

With Multiple Device Messaging (MDM), you can have one-to-one instant message (IM) conversations tracked across all devices on which you are currently signed in. If you are using a desktop client and a mobile device, both of which are MDM-enabled, messages are sent, or carbon copied, to both devices. Read notifications are also synchronized on both devices as you participate in a conversation.

MDM lets you maintain an IM conversation while moving between any of your devices. For example, if you start an IM conversation on your desktop computer, but you have to leave your desk for a meeting, you can you can continue the IM conversation on your mobile device. Clients must be signed-in to be MDM-enabled. Signed-out clients do not display sent or received IMs or notifications.

MDM supports quiet mode, which helps to conserve battery power on your mobile devices. The Jabber client turns quiet mode on automatically when the mobile client is not being used. Quiet mode is turned off when the client becomes active again.

Multiple Device Messaging Prerequisites

Instant messaging must be enabled. For details, see Group Chat and Persistent Chat Task Flow

Note If you plan to enable Multiple Device Messaging, measure deployments by the number of clients instead of the number of users as each user may have multiple Jabber clients. For example, if you have 25,000 users, and each user has two Jabber clients, your deployment requires the capacity of 50,000 users.

Configure Multiple Device Messaging

Multiple Device Messaging is enabled by default. You can use this procedure to disable the feature, or to turn it back on after it has been disabled.

Procedure

Step 1 In **Cisco Unified CM IM and Presence Administration**, choose **System** > **Service Parameters**.

Step 2 From the **Server** drop-down list, choose the IM and Presence Service Publisher node.

Step 3 From the **Service** drop-down list, choose **Cisco XCP Router (Active)**.

Step 4 From the **Enable Multi-Device Messaging** drop-down list, select either **Enabled** (the default value) or **Disabled**.

Step 5 Click **Save**.

Step 6 Restart the Cisco XCP Router service:

a) Log in to Cisco Unified IM and Presence Serviceability and choose **Tools** > **Control Center - Network Services**.

b) From the **Server** drop-down list box, select the IM and Presence publisher node.

c) Under **IM and Presence Services**, select **Cisco XCP Router** and click **Restart**.

Multiple Device Messaging Flow Use Case

This flow describes how messages and notifications are handled when a user, Alice, has MDM enabled on her laptop and mobile device.

1. Alice has a Jabber client open on her laptop, and is also using Jabber on her mobile device.
2. Alice receives an instant message (IM) from Bob.

   Her laptop receives a notification and displays a new message indicator. Her mobile device receives a new message with no notification.

Note IMs are always sent to all MDM-enabled clients. Notifications are displayed either on the active Jabber client only or, if no Jabber client is active, notifications are sent to all Jabber clients.

3. Alice chats with Bob for 20 minutes.

   Alice uses her laptop as normal to do this, while on her mobile device new messages are received and are marked as read. No notifications are sent to her mobile device.
4. When Alice receives three chat messages from a third user, Colin, Alice's devices behave as they did in step 2.
5. Alice does not respond, and closes the lid on her laptop. While on the bus home Alice receives another message from Bob.

In this case, both her laptop and mobile device receive a new message with notifications.

6. Alice opens her mobile device, where she finds the new messages sent from Bob and Colin. These messages have also been sent to her laptop.
7. Alice reads through her messages on her mobile device, and as she does so, messages are marked as read on both her laptop and on her mobile device.

Multiple Device Messaging Quiet Mode Use Case

This flow describes the steps Multiple Device Messaging uses to enable quiet mode on a mobile device.

1. Alice is using Jabber on her laptop and also on her mobile device. She reads a message from Bob and sends a response message using Jabber on her laptop.
2. Alice starts using another application on her mobile device. Jabber on her mobile device continues working in the background.
3. Because Jabber on her mobile device is now running in the background, quiet mode is automatically enabled.
4. Bob sends another message to Alice. Because Alice's Jabber on her mobile device in quiet mode, messages are not delivered. Bob’s response message to Alice is buffered.
5. Message buffering continues until one of these triggering events occur:
   - An `<iq>` stanza is received.
   - A `<message>` stanza is received when Alice has no other active clients currently operating on any other device.

Note An active client is the last client that sent either an Available presence status or an instant message in the previous five minutes.

   - The buffering limit is reached.
6. When Alice returns to Jabber on her mobile device, it becomes active again. Bob's message, which had been buffered is delivered, and Alice is able to view it.

Multiple Device Messaging Interactions and Restrictions

The following table summarizes feature interactions and restrictions with the Multiple Device Messaging (MDM) feature.

Table 1: Multiple Device Messaging Interactions and Restrictions

Feature	Interaction or Restriction
Cisco Jabber Clients	MDM is supported by all Jabber clients from version 11.7 and higher.

Feature	Interaction or Restriction
Group Chat	Group chat is available for all MDM users, who have signed in from any device.
Message Archiver	MDM is compatible with the Message Archiver feature.
Managed File Transfer	File transfer is available for all MDM users, who have signed in from any device.
Mobile and Remote Access via Expressway	For Mobile and Remote Access clients that connect to IM and Presence Service via Cisco Expressway, you must be running at least Expressway X8.8 minimum to use MDM.
Server Recovery Manager	The Multiple Device Messaging feature causes a delay with server recovery on the IM and Presence Service if failover occurs. If server failover occurs on a system where Multiple Device Messaging is configured, the failover times generally are twice as long as the times specified with the **Cisco Server Recovery Manager** service parameters.
Third-Party Clients	MDM is compatible with third-party clients that do not support the feature.

Counters for Multiple Device Messaging

Multiple Device Messaging (MDM) uses the following counters from the Cisco XCP MDM Counters Group:

Counter Name	Description
MDMSessions	The current number of MDM enabled sessions.
MDMSilentModeSessions	The current number of sessions in silent mode.
MDMQuietModeSessions	The current number of sessions in quiet mode.
MDMBufferFlushes	The total number of MDM buffer flushes.
MDMBufferFlushesLimitReached	The total number of MDM buffer flushes due to reaching the overall buffer size limit.
MDMBufferFlushPacketCount	The number of packets flushed in the last timeslice.
MDMBufferAvgQueuedTime	The average time in seconds before the MDM buffer is flushed.

Device Capacity Monitoring

When you enable Multiple Device Messaging (MDM) each user logged in from multiple device adds traffic load on the IM and Presence server. When the number of active logged in users reaches certain limit, this

results in resource shortage (memory consumption, CPU utilization) and in unexpected performance issues and failures.

The Device Capacity Monitoring feature helps address these issues by implementing additional counters to assist in monitoring the number of sessions created on the node.

The following Jabber Session Manager(JSM) sessions are created on IM&P Node:

- Composed JSM session — gets created when a user is assigned to a node.
- Active JSM session
  - On-premise User login.
  - Off-premise User login.
- Phantom JSM session — for push enabled users, which handles HA failover use cases.
- Spark Interop JSM session — for hybrid users.

The following counters are introduced to monitor the JSM sessions:

- **JsmClientSessionsActive**
- **JsmPhantomSessionsActive**
- **JsmHybridSessionsActive**

Additionally, a new counter **JSMSessionsExceedsThreshold** is introduced to monitor the JSM threshold limit, which is computed based on JSM session counters and OVA size.

If the threshold limit of this counter exceeds the default value of 80% for a period of 10 minutes, the system raises "**JSMSessionsExceedsThreshold**" alert in the Real-Time monitoring Tool (RTMT).

Configure alert value using the RTMT

You can use this procedure to configure **JSMSessionsExceedsThreshold** alert value using the RTMT.

Procedure

Step 1 Log in to **Real-Time Monitoring Tool (RTMT)**, choose **System** > **Tools** > **Alert Central**.

Step 2 Click **IM and Presence** and choose **JSMSessionsExceedsThreshold** Alert name.

Step 3 Right click on **JSMSessionsExceedsThreshold** and select **Set Alert/Properties**.

Step 4 Check the **Enable Alert** check box to enable the alert.

Step 5 Set the percentage limit for number of JSM session threshold exceed value, by default the value is 80%.

Step 6 Click **Save**.

Step 7 Set the Frequency and Schedule of the alert, By default the alert is triggered every 10 mins.

Step 8 Click **Next**.

Step 9 Click **Save**.

JSM sessions support per node

The following table lists the total number of JSM sessions that can be supported per node based on testing:

OVA Size	JSM Session Count is 1.5 times of OVA Capacity
5K OVA	7.5K

OVA Size	JSM Session Count is 1.5 times of OVA Capacity
15K OVA	22.5K
25K OVA	37.5K

Note If high availability is enabled and both nodes are in ACTIVE–ACTIVE configuration, then:

1. The total number of JSM sessions that can be supported per node would be 50% of the above mentioned capacity because there is a limitation in custom alarms that it can only be configured per node.
2. You must modify the **JSMSessionsExceedsThreshold** counter value based on HA configuration.

Suggested Action:

When a custom alert is raised, check the memory and CPU usage counters from the RTMT tool for the particular node. If memory and CPU usage counter's value exceeds the threshold limits, it is recommended to load balance the users between the IM&P nodes. Currently IM&P doesn't have a mechanism to automatically load balance users between the nodes.

User Session Report for Device Capacity Monitoring

Use this procedure to view the User Session Report. This report lets you view details of the active users logged in from multiple devices at the cluster, sub cluster, and node level.

Procedure

Step 1 Log in to **Cisco Unified IM and Presence Reporting**.

Step 2 Choose **System Reports** > **IM and Presence User Sessions Report**.

Step 3 Select the **Generate Report** (bar chart) icon in the reports window to generate the User Session Report for the current time.

Step 4 Click **OK**.

Step 5 Under the Column **Report Name**, click **IM and Presence User Sessions Report**.

Note
- This report generation may take approximately 2 or more minutes.
- This report displays the Presence Redundancy Group, Node Name, Count of users logged in from one or more devices, Total number of sessions at the cluster, sub cluster, and node level along with the date and timestamp of the report generated.

Step 6 Click **download** (green arrow) icon on the right side of the Reports window to download the User Session Report for cluster, subcluster, and node level in the CSV format.

Step 7 Click the values listed in the column **Count of users logged in from one or more devices**, to generate the detailed user based report for a particular node.

Step 8 Click **download** (green arrow) icon on the right side of the Reports window to download the detailed user level information per node in the CSV format.

Note When you hover over the column **Number of sessions**, the tooltip **device type** displays the type of device using which you have logged in.

For example, the device type can be Desktop, iPad, iPhone.