Additional Requirements

High Availability Login Profiles

Important Notes About High Availability Login Profiles

- You can use the High Availability login profile tables in this section to configure the upper and lower client re-login values for your presence redundancy group. You configure the upper and lower client login values by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.
- High Availability client login profiles apply only to single cluster deployments. High Availability client login profiles cannot configure the upper and lower client re-login values for the redundancy group if multiple clusters are present. You must perform more tests to discover High Availability client login profiles in multiple cluster deployments.
- If Debug Logging is enabled for the Cisco XCP Router service, then you should expect increased CPU usage and a decrease in the currently supported logging levels for IM and Presence Service.
- By configuring the upper and lower client re-login limits on your presence redundancy group based on the tables we provide here, you can avoid performance issues and high CPU spikes in your deployment.
- We provide a High Availability login profile for each IM and Presence Service node memory size, and for each High Availability deployment type, active/active or active/standby.
- The High Availability login profile tables are calculated based on the following inputs:
    - The lower client re-login limit is based on the Server Recovery Manager service parameter "Critical Service Down Delay", for which the default is 90 seconds. If the Critical Service Down Delay is changed then the lower limit must also change.
    - The total number of users in the presence redundancy group for Active/Standby deployments, or the node with highest number of users for Active/Active deployments.

- You must configure the upper and lower client re-login limit values on both nodes in a presence redundancy group. You must manually configure all these values on both nodes in the presence redundancy group.
- The upper and lower client re-login limit values must be the same on each node in the presence redundancy group.
- If you **rebalance** your users, you must reconfigure the upper and lower client re-login limit values based on the High Availability login profile tables.

Use High Availability Login Profile Tables

Use the High Availability login profile tables to retrieve the following values:

- **Client Re-Login Lower Limit** service parameter value
- **Client Re-Login Upper Limit** service parameter value.

Procedure

Step 1 Choose a profile table based on your virtual hardware configuration, and your High Availability deployment type.

Step 2 In the profile table, choose the number of users in your deployment (round up to the nearest value). If you have an active/standby deployment, use the node with the highest number of users.

Step 3 Based on the Number of Users value for your presence redundancy group, retrieve the corresponding lower and upper retry limits in the profile table.

Step 4 Configure the lower and upper retry limits on IM and Presence Service by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters**, and choosing **Cisco Server Recovery Manager** from the Service menu.

Step 5 Check the Critical Service Down Delay value by choosing **Cisco Unified CM IM and Presence Administration** > **System** > **Service Parameters** and choosing **Cisco Server Recovery Manager** from the **Service** Menu. The default value is 90 seconds. The lower retry limit should be set to this value.

Example High Availability Login Configurations

Example 1: 15000 Users Full UC Profile - active/active deployment

You have 3000 users in your presence redundancy group, with 2000 users on one node, and 1000 users on the second node. For an unbalanced active/active deployment, Cisco recommends you use the node with the highest number of users, in this case the node with 2000 users. Using the 15000 users full US (4 vCPU 8GB) active/active profile, you retrieve these lower and upper retry values:

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
2000	120	253

Note The upper retry limit is the approximate time (seconds) it takes for all clients to login to their backup node after a failover occurs.

Note The lower limit of 120 assumes the **Critical Service Down Delay** service parameter is set to 120.

Example 2: 5000 Users Full UC Profile - active/active deployment

You have 4700 users on each node in your presence redundancy group . Cisco recommends that you round up to the nearest value, so using the 5000 users full US (4 vCPU 8GB) active/active profile you retrieve the lower and upper retry value based on a number of users value of 5000:

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
5000	120	953

Single Cluster Configuration

500 Users Full UC (1vCPU 700MHz 2GB) Active/Active Profile

Table 1: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	187
250	120	287

500 Users Full UC (1vCPU 700MHz 2GB) Active/Standby Profile

Table 2: User Login Retry Limits for Standard Deployment (500 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	187
250	120	287
500	120	453

1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Active Profile

Table 3: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287

1000 Users Full UC (1vCPU 1500MHz 2GB) Active/Standby Profile

Table 4: User Login Retry Limits for Standard Deployment (1000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453

2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Active Profile

Table 5: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
500	120	287
1000	120	453

2000 Users Full UC (1vCPU 1500Mhz 4GB) Active/Standby Profile

Table 6: User Login Retry Limits for Standard Deployment (2000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	153
250	120	203
500	120	287
750	120	370
1000	120	453
1250	120	537
1500	120	620
1750	120	703
2000	120	787

5000 Users Full UC (4 GB 2vCPU) Active/Active Profile

Table 7: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537

5000 Users Full UC (4 GB 2vCPU) Active/Standby Profile

Table 8: User Login Retry Limits for Standard Deployment (5000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	137
500	120	203
1000	120	287
1500	120	370
2000	120	453
2500	120	537
3000	120	620
3500	120	703
4000	120	787
4500	120	870
5000	120	953

15000 Users Full UC (4 vCPU 8GB) Active/Active Profile

Attention To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

Table 9: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Active)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
7500	120	620

15000 Users Full UC (4 vCPU 8GB) Active/Standby Profile

Attention To achieve maximum client login throughput on a 15000 user system, Cisco recommends a minimum of 2.5GHz CPU clock speed.

Table 10: User Login Retry Limits for Standard Deployment (15000 Users Full UC Active/Standby)

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
Full UC		
100	120	127
500	120	153
1000	120	187
1500	120	220
2000	120	253
2500	120	287
3000	120	320
3500	120	353
4000	120	387
4500	120	420
5000	120	453
6000	120	520
7000	120	587
8000	120	653

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
9000	120	720
10000	120	787
11000	120	853
12000	120	920
13000	120	987
14000	120	1053
15000	120	1120

25000 Users Full UC (6 vCPU 16GB) Active/Active Profile

Attention To achieve maximum client login throughput on a 25000 user system, Cisco recommends a minimum of 2.8GHz CPU clock speed.

Table 11: Login rates for active /active profiles: 9 uses 45% CPU

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
100	120	131
500	120	176
1000	120	231
1500	120	287
2000	120	342
2500	120	398
3000	120	453
3500	120	509
4000	120	564
4500	120	620
5000	120	676
6000	120	787
7000	120	898
7500	120	953

Expected Number of Active Users	Lower Retry Limit	Upper Retry Limit
8000	120	1009
9000	120	1120
10000	120	1231
11000	120	1342
12000	120	1453
12500	120	1509

25000 Users Full UC (6 vCPU 16GB) Active/Standby Profile

Attention To achieve maximum client login throughput on a 25000 user system, Cisco recommends a minimum of 2.8GHz CPU clock speed.

Table 12: Login rates for active /standby profiles: 16 users 80% CPU

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
100	120	126
500	120	151
1000	120	183
1500	120	214
2000	120	245
2500	120	276
3000	120	308
3500	120	339
4000	120	370
4500	120	401
5000	120	433
6000	120	495
7000	120	558
8000	120	620
9000	120	683

Expected number of Active Users	Lower Retry Limit	Upper Retry Limit
10000	120	745
11000	120	808
12000	120	870
13000	120	933
14000	120	995
15000	120	1058
16000	120	1120
17000	120	1183
18000	120	1245
19000	120	1308
20000	120	1370
21000	120	1433
22000	120	1495
23000	120	1558
24000	120	1620
25000	120	1683

XMPP Standards Compliance

The IM and Presence Service is compliant with the following XMPP standards:

- RFC 3920 Extensible Messaging and Presence Protocol (XMPP): Core RFC 3921 Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence
  - XEP-0004 Data Forms
  - XEP-0012 Last Activity
  - XEP-0013 Flexible Offline Message Retrieval
  - XEP-0016 Privacy Lists
  - XEP-0030 Service Discovery
  - XEP-0045 Multi-User Chat
  - XEP-0054 Vcard-temp
  - XEP-0055 Jabber Search

- XEP-0060 Publish-Subscribe
- XEP-0065 SOCKS5 Bystreams
- XEP-0066 Out of Band Data Archive OOB requests
- XEP-0068 Field Standardization for Data Forms
- XEP-0071 XHTML-IM
- XEP-0082 XMPP Date and Time Profiles
- XEP-0092 Software Version
- XEP-0106 JID Escaping
- XEP-0114 Jabber Component Protocol
- XEP-0115 Entity Capabilities
- XEP-0124 Bidirectional Streams over Synchronous HTTP (BOSH)
- XEP-0126 Invisibility
- XEP-0128 Service Discovery Extensions
- XEP-0160 Best Practices for Handling Offline Messages
- XEP-0163 Personal Eventing Via PubSub
- XEP-0170 Recommended Order of Stream Feature Negotiation
- XEP-0178 Best Practices for Use of SASL EXTERNAL
- XEP-0220 Server Dialback
- XEP-0273 SIFT (Stanza Interception and Filtering Technology)

Configuration Changes and Service Restart Notifications

Whenever you need to restart a service, an **Active Notifications** popup appears. There is an **Active Notifications Summary** in the top right of the Cisco Unified CM IM and Presence Administration GUI header.

In addition, you can access an Active Notifications Listing by choosing **System** > **Notifications** From the Cisco Unified CM IM and Presence Administration interface.

Configuration Changes that Require a Restart

For many IM and Presence configuration changes and updates, you must restart the Cisco XCP Router, Cisco SIP Proxy or Cisco Presence Engine.

The following table displays the configuration changes that require a restart of any of these services. This list includes configuration changes, but does not include platform changes such as installs or upgrades.

Configurations that Require a Restart	Restart this Service
Application Listener Configuration (System > Application Listeners) Editing Application Listeners	Cisco SIP Proxy
Compliance Profile Configuration (Messaging > Compliance > Compliance Settings) (Messaging > Compliance > Compliance Profiles If you edit settings for events that are assigned to a 3rd party compliance server	Cisco XCP Router
Group Chat System Administrators (Messaging >Group Chat System Administrators) If you enable or disable this setting	Cisco XCP Router
External File Server Configuration (Messaging > External Server Setup > External File Servers) If you edit the **Host/IP Address Setting** If you regenerate the **External File Server Public Key**	Cisco XCP Router
Group Chat and Persistent Chat Configuration (Messaging > Group Chat and Persistent Chat) If a chat node cannot reach its external DB at startup, the Cisco XCP Text Conference Mgr Service is not running	Cisco XCP Router
Group Chat Server Alias Mapping (Messaging > Group Chat Server Alias Mapping) Adding a chat alias	Cisco XCP Router
ACL Configuration (System > Security > Incoming ACL) (System > Security > Outgoing ACL) Edit Incoming or Outgoing ACL Configuration	Cisco SIP Proxy
Compliance Settings Message Archiver - edit the settings	Cisco XCP Router
LDAP Server (Application > Third-Party Clients > Third-party LDAP Settings) LDAP Search - editing LDAP Search Editing the Build vCards from LDAP Editing the LDAP attribute to use for vCard FN	Cisco XCP Router

Configurations that Require a Restart	Restart this Service
Message Settings Configuration (Messaging > Settings) Editing the Enable instant message Suppress offline instant messaging	Cisco XCP Router
Microsoft RCC Configuration (Application > Microsoft RCC > Settings) Editing any of the settings on this page	Cisco SIP Proxy
Presence Gateway (Presence > Gateways) Add, edit, delete a presence gateway After you upload MS Exchange certificates	Cisco Presence engine
Presence Settings Configuration (Presence > Settings > Standard Configuration) Editing the Enable Availability Sharing setting Allow users to view the availability of other users without being prompted for approval Maximum Contact List Size (per user) Maximum Watchers	Cisco Presence Engine Cisco XCP Router
Presence Settings Configuration (Presence > Settings > Standard Configuration) Editing the **Enable user of Email address for Interdomain Federation** field	Cisco XCP Router
Partitioned Intradomain Federation Configuration Presence > Settings > Standard Configuration (check box) Presence > Intradomain Federation Setup (wizard) Enable Partitioned Intradomain Federation with LCS/OCS/Lync via the check box or via the wizard Partitioned intradomain Routing Mode - configured via the Standard Configuration window or via the wizard	Editing these settings causes automatic restart of Cisco SIP Proxy In addition, you must restart XCP Router
Proxy Configuration (Presence > Routing > Settings) Any edit to the Proxy Configuration	Cisco SIP Proxy

Configurations that Require a Restart	Restart this Service
Security Settings (System > Security > Settings) Editing any SIP security settings such as SIP Intracluster Proxy to Proxy Transport Protocol Editing any XMPP security setting	Cisco SIP Proxy (for SIP security edits) Cisco XCP Router (for XMPP security edits)
SIP Federated Domain (Presence > Interdomain Federation > SIP Federation) Add, edit, delete this configuration	Cisco XCP Router
Third-Party Compliance Service (Application > Third-Party Clients > Third-Party LDAP Servers) Edit the Hostname/IP Address, Port, Password/Confirm Password fields	Cisco XCP Router
TLS Peer Subject Configuration (System > Security > TLS Peer Subjects) Any edits on this page	Cisco SIP Proxy
TLS Context (System > Security > TLS Context Configuration) Any edits on this page	You may need to restart the associated chat server
XMPP Federation (Presence > Interdomain Federation > XMPP Federation > Settings) (Presence > Interdomain Federation > XMPP Federation > Policy) Any edits to XMPP Federation	Cisco XCP Router
Intercluster Peering (Presence Inter-clustering) Editing the intercluster peer configuration	You may be asked to restart the Cisco XCP Router (a notification appears in the top right window) in some cases
Ethernet settings (From Cisco Unified IM and Presence OS Administration, Settings > IP > Ethernet/Ethernet IPv6) Editing any ethernet settings	Causes immediate system restart
IPv6 Configuration (System > Enterprise Parameters) Editing the Enable IPv6 enterprise parameter	Cisco XCP Router Cisco SIP Proxy Cisco Presence Engine

Configurations that Require a Restart	Restart this Service
Troubleshooting If an IM and Presence publisher changes while subscriber is offline Edit the Settings > IP > Publisher setting from the subscriber	Restart subscriber node
Upgrading IM and Presence and you need to switch to previous version	Restart the system
Regenerating the cup certificate	Cisco SIP Proxy Cisco Presence Engine
Regenerate cup-xmpp	Cisco XCP Router
Regenerate cup-xmpp-s2s certificate	Cisco XCP Router
Upload new certificate	Restart relevant service for that certificate. For Cup-trust certificates, restart the Cisco SIP Proxy
Remote Audit Log Transfer Protocol if you run any of the utils remotesyslog set protocol * CLI commands	Restart the node
If you get any of the following alerts: • PEIDSQueryError • PEIDStoIMDBDatabaseSyncError • PEIDSSubscribeError • PEWebDAVInitializationFailure	It's recommended to restart Cisco Presence Engine
If you get any of the following alerts: • • XCPConfigMgrJabberRestartRequired • XCPConfigMgrR2RPasswordEncryptionFailed • XCPConfigMgrR2RRequestTimedOut • XCPConfigMgrHostNameResolutionFailed	It's recommended to restart Cisco XCP Router
PWSSCBInitFailed	It's recommended to restart Cisco SIP Proxy

Configurations that Require a Restart	Restart this Service
Editing any of the Exchange Service Parameters • Microsoft Exchange Notification Port • Calendar Spread • Exchange Timeout (seconds) • Exchange Queue • Exchange Threads • EWS Status Frequency	Cisco Presence Engine
Upload Exchange Certificates	Cisco SIP Proxy Cisco Presence Engine
Installing locales	Restart the IM and Presence Service
Create new MSSQL external database	Cisco XCP Router
Editing external database configuration	Cisco XCP Router
Merging external database	Cisco XCP Router
Configuring TLS Peer Subjects	Cisco SIP Proxy
Configuring Peer Authentication TLS Context	Cisco SIP Proxy
Editing the following Cisco SIP Proxy Service Parameters: • CUCM Domain • Server Name (supplemental) • HTTP Port • Stateful Server (transaction Stateful) • Persist TCP Connections • Shared memory size (bytes) • Federation Routing IM/P FQDN • Microsoft Federation User-Agent Headers (comma-delimited)	Cisco SIP Proxy
Edit the **Routing Communication Type** service parameter	Cisco XCP Router
Editing the IM address scheme	Cisco XCP Router
Assign a default domain	Cisco XCP Router
Deleting or removing a node from the cluster	Cisco XCP Router

Configurations that Require a Restart	Restart this Service
Any edit to a parameter that affects the Cisco XCP router requires you to restart the Cisco XCP router	Cisco XCP Router
Routing Communication Type service parameters	Cisco XCP Router
Editing either of the Cisco XCP File Transfer Manager service parameters: • **External File Server Available Space Lower Threshold** • **External File Server Available Space Upper Threshold**	Cisco XCP Router
Edit the **Enable Mulitple Device Messaging** service parameter	Cisco XCP Router
Editing the **Maximum number of logon sessions per user** service parameter	Cisco XCP Router
Updating the `install_dir /data/pg_hba.conf` or `install_dir /data/postgresql.conf` config files on the external database	Cisco XCP Router
Migration utilities: • Editing the **Allow users to view the availability of other users without being prompted for approval** setting in the Presence Settings window. • Editing the **Maximum Contact Lists Size (per user)** and **Maximum Watchers (per user**) setting in the Presence Settings configuration window.	Cisco XCP Router
Deleting or removing a node from a cluster	Cisco XCP Router

Additional Requirements