Cisco IM and Presence Service Configuration Report

Sample Report IM and Presence

As-Built Documentation for project

Document Information - Universal
Version Status

Release Number	Date	Reason for Version
1.0	October 21, 2019	Release

Client Information

Prepared for:	Large Company Inc.
Name:	H. Boss
Title:	CEO
Address:	Corporate Way
Telephone:	1 (555) 56987424
Email:	hboss@largecompany.com

Presenter Information

Prepared by:	Config Reports Ltd.
Name:	Jennifer SMITH
Title:	Ms.
Address:	22 Main Street
Telephone:	123456787
Email:	JSmith@email.com

Table of Content

1 Report Information

This configuration report contains the configuration objects for the IM and Presence cluster.

1.1 Report Generation

This configuration report for Cisco Unified CM IM and Presence cluster has the following details:

Report Info	
Report Date	21/10/2019 2:42:52 PM
Report generated for	Sample Report IM and Presence
Description	As-Built Documentation for project
Server Info	
IMP version	12.5.1.10000(6)
IMP IP	10.5.1.122
Report Settings	
Report Type	Direct Report
Visual Style	Blu Dark.css
Report Content	All objects
Template HTML	CUPSreportTemplate.htm
Template Word	Gears-Blue-universal.doc
Report Tool Info	
Report Tool Version	12.0.19 / 19 Oct 2019
Report Tool License	Licensed [Prof all]

2 System

The System section contains the following items:

- Server
- Services
- Status
- Application Listeners
- Security
- Settings
- Incoming ACL
- Outgoing ACL
- TLS Context Configuration
- TLS Peer Subjects
- Service Parameters
- Enterprise Parameters

2.1 System - Server

The following IM and Presence servers are present in this cluster:

Server				
Host Name/IP Address	**Node Type**	**Node Role**	**MAC Address**	**Description**
10.5.1.120	Publisher	Voice		
10.5.1.122	Publisher	Presence		

2.2 System - Status

The IM and Presence system status shows the Sync Information and System Information. The system status displays the IP address of the publisher server and when the sync occurred.

System Information displays the following read-only fields:

- Number of end users
- Number of phone devices
- Number of licensed IM and Presence end users
- Number of licensed Cisco Unified Personal Communicator end users
- Number of assigned Microsoft Office Communicator end users
- Number of end users associated with an inter-cluster peer

Cisco Unified Presence System Status	
Name	Value
Publisher:	10.5.1.120
Sync Status:	Completed 2019-09-16 00:35:43
No. End users:	119
No. Phone Devices:	13
No. Licensed Cisco Unified Presence (CUP) End users:	2
No. Licensed Cisco Unified Personal Communicator (CUPC) End users:	2
No. Assigned Microsoft Office Communicator (MOC) End users:	0
No. End users Associated with Intercluster Peer: 10.5.1.152	1

2.3 System - CUCM Publisher

The following Cisco Unified Communications Manager (CUCM) Publisher is configured. Data will be synchronized from the publisher to the IM and Presence Service cluster.

CUCM Publisher Configuration	
Name	Value
CUCM Publisher Hostname	CUCM120
CUCM Publisher IP Address	10.5.1.120
AXL Username	admin
Sync Status	Completed 2019-09-16 00:35:43
CUCM Version	12.5.1.10000(22)

2.4 System - Services

The following services are present on this server:

Services					
Server Name	Node Type	Service Name	Status	Activation Status	Start Time
10.5.1.122	Publisher	A Cisco DB	Started	Activated	Mon Sep 16 00:25:38 2019
10.5.1.122	Publisher	A Cisco DB Replicator	Started	Activated	Mon Sep 16 00:25:39 2019
10.5.1.122	Publisher	Cisco AMC Service	Started	Activated	Mon Sep 16 00:26:12 2019
10.5.1.122	Publisher	Cisco AXL Web Service	Started	Activated	Mon Sep 16 00:26:22 2019
10.5.1.122	Publisher	Cisco Audit Event Service	Started	Activated	Mon Sep 16 00:26:13 2019
10.5.1.122	Publisher	Cisco CDP	Started	Activated	Mon Sep 16 00:25:54 2019
10.5.1.122	Publisher	Cisco CDP Agent	Started	Activated	Mon Sep 16 00:25:48 2019
10.5.1.122	Publisher	Cisco CallManager Serviceability	Started	Activated	Mon Sep 16 00:30:46 2019
10.5.1.122	Publisher	Cisco CallManager Serviceability RTMT	Started	Activated	Mon Sep 16 00:30:46 2019
10.5.1.122	Publisher	Cisco Certificate Expiry Monitor	Started	Activated	Mon Sep 16 00:26:05

Services					
Server Name	**Node Type**	**Service Name**	**Status**	**Activation Status**	**Start Time**
					2019
10.5.1.122	Publisher	Cisco Client Profile Agent	Started	Activated	Mon Sep 16 00:26:23 2019
10.5.1.122	Publisher	Cisco Config Agent	Started	Activated	Mon Sep 16 00:26:16 2019
10.5.1.122	Publisher	Cisco DRF Local	Started	Activated	Mon Sep 16 00:26:04 2019
10.5.1.122	Publisher	Cisco Database Layer Monitor	Started	Activated	Mon Sep 16 00:25:40 2019
10.5.1.122	Publisher	Cisco IM and Presence Admin	Started	Activated	Mon Sep 16 00:26:19 2019
10.5.1.122	Publisher	Cisco IM and Presence Data Monitor	Started	Activated	Mon Sep 16 00:25:59 2019
10.5.1.122	Publisher	Cisco Intercluster Sync Agent	Started	Activated	Mon Sep 16 00:26:03 2019
10.5.1.122	Publisher	Cisco Log Partition Monitoring Tool	Started	Activated	Mon Sep 16 00:25:53 2019
10.5.1.122	Publisher	Cisco Login Datastore	Started	Activated	Mon Sep 16 00:25:41 2019
10.5.1.122	Publisher	Cisco Management Agent Service	Started	Activated	Mon Sep 16 00:26:14 2019
10.5.1.122	Publisher	Cisco OAM Agent	Started	Activated	Mon Sep 16 00:26:17 2019
10.5.1.122	Publisher	Cisco Presence Datastore	Started	Activated	Mon Sep 16 00:26:09 2019
10.5.1.122	Publisher	Cisco Presence Engine	Started	Activated	Tue Oct 8 02:12:28 2019
10.5.1.122	Publisher	Cisco RCC Device Selection Service	Started	Activated	Mon Sep 16 00:26:20 2019
10.5.1.122	Publisher	Cisco RIS Data Collector	Started	Activated	Mon Sep 16 00:26:11 2019
10.5.1.122	Publisher	Cisco RTMT Reporter Servlet	Started	Activated	Mon Sep 16 00:30:46 2019
10.5.1.122	Publisher	Cisco Route Datastore	Started	Activated	Mon Sep 16 00:25:42 2019
10.5.1.122	Publisher	Cisco SIP Proxy	Started	Activated	Tue Oct 8 02:45:31 2019
10.5.1.122	Publisher	Cisco SIP Registration Datastore	Started	Activated	Mon Sep 16 00:26:10 2019
10.5.1.122	Publisher	Cisco Server Recovery Manager	Started	Activated	Mon Sep 16 00:26:00 2019
10.5.1.122	Publisher	Cisco Sync Agent	Started	Activated	Mon Sep 16 00:33:33 2019
10.5.1.122	Publisher	Cisco Syslog Agent	Started	Activated	Mon Sep 16 00:25:49 2019
10.5.1.122	Publisher	Cisco Tomcat	Started	Activated	Mon Sep 16 00:25:43 2019
10.5.1.122	Publisher	Cisco Tomcat Stats Servlet	Started	Activated	Mon Sep 16 00:26:08 2019
10.5.1.122	Publisher	Cisco Trace Collection Service	Started	Activated	Mon Sep 16 00:26:07 2019
10.5.1.122	Publisher	Cisco Trace Collection Servlet	Started	Activated	Mon Sep 16 00:26:06 2019
10.5.1.122	Publisher	Cisco XCP Authentication Service	Started	Activated	Tue Oct 8 03:29:30 2019
10.5.1.122	Publisher	Cisco XCP Config Manager	Started	Activated	Mon Sep 16 00:26:01 2019

Services					
Server Name	**Node Type**	**Service Name**	**Status**	**Activation Status**	**Start Time**
10.5.1.122	Publisher	Cisco XCP Connection Manager	Started	Activated	Tue Oct 8 03:29:30 2019
10.5.1.122	Publisher	Cisco XCP Directory Service	Started	Activated	Tue Oct 8 03:29:30 2019
10.5.1.122	Publisher	Cisco XCP Router	Started	Activated	Mon Sep 16 00:26:18 2019
10.5.1.122	Publisher	Cisco XCP XMPP Federation Connection Manager	Started	Activated	Thu Oct 10 00:44:30 2019
10.5.1.122	Publisher	Host Resources Agent	Started	Activated	Tue Sep 17 06:29:19 2019
10.5.1.122	Publisher	MIB2 Agent	Started	Activated	Mon Sep 16 00:25:45 2019
10.5.1.122	Publisher	Platform Administrative Web Service	Started	Activated	Mon Sep 16 00:26:21 2019
10.5.1.122	Publisher	Platform Communication Web Service	Started	Activated	Mon Sep 16 00:26:15 2019
10.5.1.122	Publisher	SNMP Master Agent	Started	Activated	Tue Sep 17 06:29:14 2019
10.5.1.122	Publisher	SOAP -Log Collection APIs	Started	Activated	Mon Sep 16 00:30:46 2019
10.5.1.122	Publisher	SOAP -Performance Monitoring APIs	Started	Activated	Mon Sep 16 00:30:46 2019
10.5.1.122	Publisher	SOAP -Real-Time Service APIs	Started	Activated	Mon Sep 16 00:30:46 2019
10.5.1.122	Publisher	System Application Agent	Started	Activated	Mon Sep 16 00:25:47 2019
10.5.1.122	Publisher	Cisco Bulk Provisioning Service	Stopped	Deactivated	< None >
10.5.1.122	Publisher	Cisco Serviceability Reporter	Stopped	Deactivated	< None >
10.5.1.122	Publisher	Cisco XCP File Transfer Manager	Stopped	Deactivated	< None >
10.5.1.122	Publisher	Cisco XCP Message Archiver	Stopped	Deactivated	< None >
10.5.1.122	Publisher	Cisco XCP SIP Federation Connection Manager	Stopped	Deactivated	< None >
10.5.1.122	Publisher	Cisco XCP Text Conference Manager	Stopped	Deactivated	< None >
10.5.1.122	Publisher	Cisco XCP Web Connection Manager	Stopped	Deactivated	< None >

2.5 System - Application Listeners

You can configure application listeners for the SIP proxy server, presence engine, and profile agent. The system binds each application listener to a specific address and port combination. If you choose TLS protocol, you must also choose a TLS context.

Transport Listener					
Name	**Port**	**Listener Type**	**Service**	**Transport Type**	**TLS Context**
ANewListenerForTesting	5059	SIP	Cisco SIP Proxy	UDP	
Default Cisco IM and Presence Service HTTP Listener	8082	HTTP	Cisco SIP Proxy	TCP	
Default Cisco IM and Presence Service HTTPS Listener	8083	HTTPS	Cisco SIP Proxy	TLS	Default_Cisco_UP_3rd_Party_API_TLS_Context
Default Cisco IM and Presence Service XMPP Federation Listener	5269	XMPP	Cisco XCP XMPP Federation Connection Manager	TCP	

Transport Listener					
Name	Port	Listener Type	Service	Transport Type	TLS Context
Default Cisco Presence Engine TCP Listener	5070	SIP	Cisco Presence Engine	TCP	
Default Cisco Presence Engine UDP Listener	5070	SIP	Cisco Presence Engine	UDP	
Default Cisco SIP Proxy TCP Listener	5060	SIP	Cisco SIP Proxy	TCP	
Default Cisco SIP Proxy TLS Listener - Peer Auth	5062	SIP	Cisco SIP Proxy	TLS	Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context
Default Cisco SIP Proxy TLS Listener - Server Auth	5061	SIP	Cisco SIP Proxy	TLS	Default_Cisco_UP_SIP_Proxy_Auth_TLS_Context
Default Cisco SIP Proxy UDP Listener	5060	SIP	Cisco SIP Proxy	UDP	

2.6 Security

The Security section contains the following items:

- Settings
- Incoming ACL
- Outgoing ACL
- TLS Context Configuration
- TLS Peer Subjects

2.6.1 Security - Settings

This section contains settings for secure modes of XMPP traffic, the preferred transport protocol for SIP intracluster traffic, and the domain name for the XMPP server-to-server certificate.

Security Settings	
Name	Value
Enable XMPP Client to IM/P Service Secure Mode	Y
Enable XMPP Router-to-Router Secure Mode	N
Enable Web Client to IM/P Service Secure Mode	Y
Enable Wildcards in XMPP Federation Security Certificates	N
SIP Intra-cluster Proxy-to-Proxy Transport Protocol	TCP

2.6.2 Security - Incoming ACL

The Access Control List (ACL) configure patterns that control which hosts and domains can access Cisco Unified Presence.

Configure an address which will be added to the SIP Proxy list of allowed incoming addresses. Note: any address added to this list will bypass digest authentication. By default, the behavior is to deny all incoming requests.

Incoming ACL Entry	
Address Pattern	Description
10.5.1	Allow from our IP range
10.5.1.120	System Generated Allow Rule
10.5.1.122	System Generated Allow Rule
10.5.1.152	System Generated Allow Rule
microsoft.com	System Generated Allow Rule

2.6.3 Security - Outgoing ACL

The Outgoing Access Control List (ACL) configures patterns that control which outgoing hosts and domains can have access to the network from Cisco Unified Presence.

Configure an address which will be added to the SIP Proxy list of allowed outgoing addresses. Note: any address added to this list will bypass digest authentication. By default, the behavior is to deny all outgoing requests.

Outgoing ACL Entry	
Address Pattern	Description
10.5.1	Allow to our IP range
10.5.1.120	System Generated Allow Rule
10.5.1.122	System Generated Allow Rule
10.5.1.152	System Generated Allow Rule

2.6.4 Security - TLS Context Configuration

Each transport listener can have a single associated transport layer security (TLS) context, and each TLS context can have multiple ciphers and peer subjects.

TLS context configuration enables you to map ciphers and peer subjects to a transport listener.

TLS Context Configuration	
Name	Configuration
Default_Cisco_UP_3rd_Party_API_TLS_Context	**TLS Context Information**
	Description	Default TLS context for Cisco 3rd Party API specifying an authorization policy of Peer
	Authorization Policy	Server
	Disable Empty TLS Fragments	N
	TLS Cipher Mapping
	Selected TLS Ciphers	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_WITH_RSA_AES_128_CBC_SHA TLS_WITH_RSA_AES_256_CBC_SHA
	TLS Peer Subject Mapping
	Selected TLS Peer Subjects	
Default_Cisco_UP_SIP_Proxy_Auth_TLS_Context	**TLS Context Information**
	Description	Default TLS context for Cisco SIP Proxy specifying an authorization policy of Server
	Authorization Policy	Server
	Disable Empty TLS Fragments	N
	TLS Cipher Mapping
	Selected TLS Ciphers	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_WITH_RSA_AES_128_CBC_SHA TLS_WITH_RSA_AES_256_CBC_SHA
	TLS Peer Subject Mapping
	Selected TLS Peer Subjects	
Default_Cisco_UP_SIP_Proxy_Peer_Auth_TLS_Context	**TLS Context Information**
	Description	Default TLS context for Cisco SIP Proxy specifying an

TLS Context Configuration	
Name	**Configuration**

		authorization policy of Peer
	Authorization Policy	Peer
	Disable Empty TLS Fragments	N
	TLS Cipher Mapping	
	Selected TLS Ciphers	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_WITH_RSA_AES_128_CBC_SHA TLS_WITH_RSA_AES_256_CBC_SHA
	TLS Peer Subject Mapping	
	Selected TLS Peer Subjects	NewPeerSubjectName

2.6.5 Security - TLS Peer Subjects

TLS peer subject configuration enables you to create and modify peer subjects that you can associate with a transport listener.

TLS Peer Subjects	
Name	**Description**
NewPeerSubjectName	This is just to test reports

2.7 System - Service Parameters

The following are the service parameters for particular services, per server:

Please note that only the common clusterwide parameters are listed as not all parameters can be retrieved.

Service Parameters - Clusterwide Parameters (Parameters that apply to all servers)		
Service	**Parameter Name**	**Parameter Value**
Cisco AMC Service	Primary Collector	10.5.1.120
Cisco AMC Service	Failover Collector	10.5.1.122
Cisco AMC Service	Amc Collection Enabled	T
Cisco AMC Service	Amc Collection Polling Rate	30
Cisco AMC Service	Amc Link Service Sync Up Period	60
Cisco AMC Service	RMI Registry Port	1099
Cisco AMC Service	RMI Object Port	1090
Cisco AMC Service	Alert Mgr Enabled	T
Cisco AMC Service	Logger Enabled	T
Cisco Bulk Provisioning Service	Default BPS Job Processing Option	1
Cisco Bulk Provisioning Service	Default BPS Job Processing Time	
Cisco Bulk Provisioning Service	Default BPS Throttling Limit	1000
Cisco Bulk Provisioning Service	BPS Log File Location	/var/log/active/cm/log/bps/
Cisco Bulk Provisioning Service	Stop BPS Job Processing	F
Cisco Config Agent	Heart Beat Interval	60
Cisco Config Agent	Connect Timeout	30
Cisco Config Agent	Max Network Outage	240

Service Parameters - Clusterwide Parameters (Parameters that apply to all servers)		
Service	**Parameter Name**	**Parameter Value**
Cisco Config Agent	Heart Beat Port	8600
Cisco Config Agent	Offline Message Heart Beat Interval	60
Cisco Config Agent	Max Offline Message Time To Live	14
Cisco Config Agent	Roster Heart Beat Interval	60
Cisco Config Agent	Max Roster Entry Time To Live	30
Cisco Database Layer Monitor	Device Name Validation Enabled	T
Cisco Database Layer Monitor	CDR Purge Time	00:00
Cisco Database Layer Monitor	CDR Purge Window	12
Cisco Database Layer Monitor	Table Out Of Sync	0
Cisco Database Layer Monitor	Sort End User Locale	1
Cisco Database Layer Monitor	Axl Change Notification	1
Cisco Database Layer Monitor	Axl Change Notification Queue Size	20000
Cisco Database Layer Monitor	Valid Namespace	T
Cisco Database Layer Monitor	SPL Trace	1
Cisco Database Layer Monitor	SPL App Trace Level	1
Cisco Database Layer Monitor	Maintenance Task Trace	0
Cisco Database Layer Monitor	Enable AXL Encoding Info	F
Cisco Database Layer Monitor	Check For Namespace In Tag	T
Cisco Database Layer Monitor	Validate Service URL	T
Cisco Database Layer Monitor	Replication Monitor Timeout	1800
Cisco Database Layer Monitor	Maximum Inactive Period	0
Cisco Database Layer Monitor	Disable User	0
Cisco IM and Presence Data Monitor	Eu Watcher Basic Check Interval	30
Cisco Intercluster Sync Agent	Enable Auto Recovery For IC Peer Periodic Syncing Failure	1
Cisco Presence Engine	Presence Viewer Photo URI	MyPhotoUri
Cisco Presence Engine	Messaging Port	50000
Cisco Presence Engine	Aggregate Shared Lines	On
Cisco Presence Engine	Cupc Tuple ID	cisco-upc
Cisco Presence Engine	Client Emulation Resource Name	composed
Cisco Presence Engine	Notify Body Size	180000
Cisco Presence Engine	Presence Change Throttle Rate	50
Cisco Presence Engine	Calendar Spread	50
Cisco Presence Engine	Exchange Timeout	3

Service Parameters - Clusterwide Parameters (Parameters that apply to all servers)		
Service	**Parameter Name**	**Parameter Value**
Cisco Presence Engine	Exchange Queue	2200
Cisco Presence Engine	Exchange Threads	60
Cisco Presence Engine	EWS Status Frequency	60
Cisco Presence Engine	Office365 Calendar Information Pull Interval	60
Cisco RIS Data Collector	Ris Cluster Tcp Port	2555
Cisco RIS Data Collector	Ris Client Tcp Port	2556
Cisco RIS Data Collector	Ris Client Timeout	30
Cisco RIS Data Collector	Ris Cleanup Time Ofthe Day	22:00
Cisco RIS Data Collector	Ris Unused CM Device Store Period	3
Cisco RIS Data Collector	Ris Unused CTI Device Store Period	1
Cisco RIS Data Collector	Ris Max Num Unused CTI Records	3000
Cisco RIS Data Collector	Ris TLC Throttle Enable	T
Cisco RIS Data Collector	Ris TLCIO Throttle Limit	10
Cisco RIS Data Collector	Ris TLCCPU Throttle Limit	80
Cisco RIS Data Collector	Ris TLC Throttle Poll Rate	250
Cisco RIS Data Collector	Ris TLCSFTP Keepalive Delay	5000
Cisco RIS Data Collector	Ris System Access Max Processes Threads	2500
Cisco SIP Proxy	Virtual IP Address	
Cisco SIP Proxy	SR V_ Cluster Name	
Cisco SIP Proxy	CUCM Domain	lab.test
Cisco SIP Proxy	Server Name	
Cisco SIP Proxy	Port	8081
Cisco SIP Proxy	Stateful Server	On
Cisco SIP Proxy	Server Type	Proxy
Cisco SIP Proxy	Start Servers	20
Cisco SIP Proxy	Min Spare Servers	20
Cisco SIP Proxy	Max Spare Servers	20
Cisco SIP Proxy	Max Clients	20
Cisco SIP Proxy	Max Invite Retx Count	3
Cisco SIP Proxy	Max Non Invite Retx Count	6
Cisco SIP Proxy	Max Requests Per Child	1000000
Cisco SIP Proxy	Sip Tcp Max Connect Timeout	10000
Cisco SIP Proxy	Sip Tcp Reuse Connection	Off
Cisco SIP Proxy	Persist TCP Connections	On
Cisco SIP Proxy	Shared Memory Size	512000000
Cisco SIP Proxy	Proxy Address Resolution Type	IP
Cisco SIP Proxy	Add Record Route	On
Cisco SIP Proxy	Add Transport In Record Route	t
Cisco SIP Proxy	Sip Resolve Local Contacts In	Off

Service Parameters - Clusterwide Parameters (Parameters that apply to all servers)		
Service	Parameter Name	Parameter Value
	Redirect Mode	
Cisco SIP Proxy	Recursive	On
Cisco SIP Proxy	Numeric Username Interpretation	E164_IP
Cisco SIP Proxy	Numeric Username Character Set	+0123456789.-()#*
Cisco SIP Proxy	A Record_ IP Addr	On
Cisco SIP Proxy	Allow NAPT Rlookup	On
Cisco SIP Proxy	Transport Pref Order	TLS_TCP_UDP
Cisco SIP Proxy	Sip Route Hdr Transport Type	UDP
Cisco SIP Proxy	Diff Serv Value	0x60
Cisco SIP Proxy	Allow Sip Tls Conversion To Sip	On
Cisco SIP Proxy	Sip Tls Session Timeout	300
Cisco SIP Proxy	Max MTU Size	1300
Cisco SIP Proxy	Contact Failover_ On All But	481,487
Cisco SIP Proxy	Cisco_ Numexpand	On
Cisco SIP Proxy	Num Expand Auth User Name	On
Cisco SIP Proxy	Cisco_ Routing	On
Cisco SIP Proxy	Cisco_ Routing_ Use_ Domain_ Routing	On
Cisco SIP Proxy	Cisco_ Route_ Fail	On
Cisco SIP Proxy	Route Embed Template1	74..78xxxxx*
Cisco SIP Proxy	Route Embed Template2	73..78xxxx*
Cisco SIP Proxy	Route Embed Template3	
Cisco SIP Proxy	Route Embed Template4	
Cisco SIP Proxy	Route Embed Template5	
Cisco SIP Proxy	Privacy	On
Cisco SIP Proxy	Privacy With PAI	On
Cisco SIP Proxy	Privacy With RPID	Off
Cisco SIP Proxy	Privacy With Diversion	Off
Cisco SIP Proxy	Privacy Use PAI Domain	On
Cisco SIP Proxy	Authentication	On
Cisco SIP Proxy	Method List	INVITE,REGISTER,MESSAGE,PUBLISH,NOTIFY,SUBSCRIBE
Cisco SIP Proxy	Sip T1 In Ms	500
Cisco SIP Proxy	Sip T2 In Ms	4000
Cisco SIP Proxy	Sip T3 In Ms	60000
Cisco SIP Proxy	Sip T4 In Ms	32000
Cisco SIP Proxy	Federation Routing CUPFQDN	IMP122.lab.test-public.lab.test
Cisco SIP Proxy	Default Federation Routing Domain	aol.com
Cisco SIP Proxy	Microsoft Fed Agent Headers	Microsoft,UCCAPI,LCC,RTC,UCCP
Cisco SIP Proxy	IM Gateway Status	On
Cisco SIP Proxy	IM Gateway Timeout	600
Cisco SIP Proxy	IM Gateway Err Msg	Your IM could not be delivered.
Cisco Server Recovery Manager	Service Port	21999
Cisco Server Recovery Manager	Admin Rpc Port	20075
Cisco Server Recovery Manager	Critical Service Down Delay	90
Cisco Server Recovery	Enable Automatic Fallback	F

Service Parameters - Clusterwide Parameters (Parameters that apply to all servers)		
Service	**Parameter Name**	**Parameter Value**
Manager		
Cisco Server Recovery Manager	Init Keep Alive Timeout	120
Cisco Server Recovery Manager	Keep Alive Timeout	60
Cisco Server Recovery Manager	Keep Alive Interval	15
Cisco Serviceability Reporter	RTMT Reporter Node	10.5.1.120
Cisco Serviceability Reporter	RTMT Report Generation Time	30
Cisco Serviceability Reporter	RTMT Report Deletion Age	7
Cisco Sync Agent	Forced Sync	F
Cisco Sync Agent	Num Of Rows Grabbed Each Time	2000
Cisco Sync Agent	IM Presence Domains Mode	Automatic
Cisco XCP Connection Manager	Connection Byte Limit Option	F
Cisco XCP Connection Manager	Max Accepted Packet Size	20000
Cisco XCP File Transfer Manager	Aft-extfs-freespace-lower	10
Cisco XCP File Transfer Manager	Aft-extfs-freespace-upper	15
Cisco XCP Message Archiver	Max-queue-size	100000
Cisco XCP Router	R2 R_routing_enabled	t
Cisco XCP Router	Router-db-poolsize	11
Cisco XCP Router	Max-jsmdb-requests	1000
Cisco XCP Router	Resume-jsmdb-requests	500
Cisco XCP Router	Max-sessions	10
Cisco XCP Router	Enable-stream-management	t
Cisco XCP Router	Max-stream-management-timeout	60
Cisco XCP Router	Max-stream-management-buffer-size	100
Cisco XCP Router	Stream-management-req-ack-rate	5
Cisco XCP Router	Enable-multi-device-messaging	t
Cisco XCP Router	Enable-push-ha	t
Cisco XCP SIP Federation Connection Manager	Max-sockets-sip	1000
Cisco XCP SIP Federation Connection Manager	Cm-thread-count-sip	3
Cisco XCP SIP Federation Connection Manager	Connect-attempts-sip	10
Cisco XCP SIP Federation Connection Manager	Connect-attempts-delay-secs-sip	30
Cisco XCP SIP Federation Connection Manager	Sipgw-thread-count-xmppout-messages	3

Service Parameters - Clusterwide Parameters (Parameters that apply to all servers)		
Service	**Parameter Name**	**Parameter Value**
Cisco XCP SIP Federation Connection Manager	Sipgw-thread-count-sip-processing	3
Cisco XCP SIP Federation Connection Manager	Sipgw-max-subscriptions	200000
Cisco XCP SIP Federation Connection Manager	Sipgw-max-im-sessions	25000
Cisco XCP Text Conference Manager	Max-db-queue-size	100000
Cisco XCP Web Connection Manager	Http-binding-path-handled	/httpbinding
Cisco XCP XMPP Federation Connection Manager	Max-sockets-xmpp	1000
Cisco XCP XMPP Federation Connection Manager	Cm-thread-count-xmpp	3
Cisco XCP XMPP Federation Connection Manager	Connect-attempts-xmpp	10
Cisco XCP XMPP Federation Connection Manager	Connect-attempts-delay-secs-xmpp	30
Cisco XCP XMPP Federation Connection Manager	Keepalive	0
Cisco XCP XMPP Federation Connection Manager	Keepalive-interval	60
Cisco XCP XMPP Federation Connection Manager	Keepalive-text	keepalive
Cisco XCP XMPP Federation Connection Manager	Xmppdin-idle-timeout-secs	3600
Cisco XCP XMPP Federation Connection Manager	Dialback-timeout	30
Cisco XCP XMPP Federation Connection Manager	Xmppdout-idle-timeout-secs	3600

2.8 System - Enterprise Parameters

Enterprise parameters provide default settings that apply to all devices and services in the same cluster. A cluster is a set of servers that share the same database. When you install a new server, it uses the enterprise parameters to set the initial values of its device defaults.

You cannot add or delete enterprise parameters, but you can update existing enterprise parameters.

Enterprise Parameters	
Parameter Name	**Parameter Value**
Cluster ID	StandAloneCluster
Max Number Device Level Trace	12
Enable Trace Compression	0
DSCP For SCCP Phone Services	40
DSCP For SCCP Phone Config	96

Enterprise Parameters	
Parameter Name	**Parameter Value**
DSCP For Cm2 Dvce	96
Connection Monitor Duration	120
Auto Registration Phone Protocol	0
Auto Registration Legacy Mode	F
Phone Template Selection	1
BLF For Call Lists	1
Advertise G722 Codec	1
Phone Personalization	0
Phone Service Display	0
Feature Control Policy	f5971ce3-43fd-0c88-6673-7892a22a3b47
Wifi Hotspot Profile	53e42ff1-d739-204a-19d7-c060f60ba8c4
IMS Inter Operator Id	IMS Inter Operator Identification
URI Lookup Policy	0
CCM Admin Max Items In List	250
CCM Admin Max Items In Lookup	1000
CCM Admin Enable Dependency Records	T
Auto Select DN On Any Partition	0
CCM User Options Portal Default Server	
CCM User Show Speed Dial Settings	T
CCM User Show IP Phone Services Settings	T
CCM User Show Ring Settings	F
CCM User Show Message Waiting Lamp Policy	T
CCM User Show History Settings	T
CCM User Show Personal Address Book	T
CCM User Show Line Text Settings	F
CCM User Show Online Guide	T
CCM User Show Mobility Features	T
CCM User Show Directory	T
CCM User Show Calendar Preference	T
CCM User Show Phone Locale	T
CCM User Show Change Password	T
CCM User Show Change Pin	T
CCM User Show Call Forward	1
CCM User Show Voicemail IVR Option	T
CCM User Show Conferencing Scheduler	T
CCM User Show Video Conferencing Scheduler	1
CCM User Show Download	T
CCM User Display Name	T
CCM User Show Phones Ready To Activate	T
End User Directory URI Partition Alias	4d5461af-f3d8-cddf-072e-54e8412e8a9e
CDR Flat File Interval	1
Default Network Locale	64
Default User Locale	1
MLPP Domain Identifier	c80cafe0-af65-43d6-a1f1-225ad998bd26
MLPP Indication Status	Off
MLPP Preemption Setting	Disabled
Precedence Alternate Party Timeout	30
Use Standard VM Handling For Precedence Calls	F
Confidential Access Level Policy	F

Enterprise Parameters	
Parameter Name	**Parameter Value**
Confidential Access Level Enforcement Level	0
Confidential Access Level Value For Warning	0
Confidential Access Level Warning Message Text	
Confidential Access Level Failure Message Text	CAL MISMATCH
Cluster Security Mode	0
Cluster SIPO Auth Mode	0
LBM Security Mode	0
CAPF Phone Port	3804
CAPF Operation Duration	10
Endpoint Encryption Algorithms	0
TFTP File Signature Algorithm	1
Cache Control	T
Auth Method For Browser Access	1
TLS Cipher Preference	1
SRTP Cipher Selection	0
HTTPS Cipher Selection	1
Trusted Servers	
Terminate User Session	1
Certificate Validity Check	0
Certificate Validity Check Frequency	24
Roll Back To Pre Grayback	F
URL Authentication	http://10.5.1.120:8080/ccmcip/authenticate.jsp
URL Directories	http://10.5.1.120:8080/ccmcip/xmldirectory.jsp
URL Idle	
URL Idle Time	
URL Information	http://10.5.1.120:8080/ccmcip/GetTelecasterHelpText.jsp
URL Messages	
URL Proxy	
URL Services	http://10.5.1.120:8080/ccmcip/getservicesmenu.jsp
Secure Authentication URL	
Secure Directory URL	https://10.5.1.120:8443/ccmcip/xmldirectory.jsp
Secure UDS Users Access URL	https://10.5.1.120:8443/cucm-uds/users
Secure Idle URL	
Secure Information URL	https://10.5.1.120:8443/ccmcip/GetTelecasterHelpText.jsp
Secure Messages URL	
Secure Services URL	https://10.5.1.120:8443/ccmcip/getservicesmenu.jsp
Enable All User Search	T
User Search Limit	64
Numberof Digitsto Match	4
CCMPD Session Timeout	86400
Allowed Perfmon Queries Per Minute	50
Allowed Ris Queries Per Minute	15
Perfmon Queue Limit	100
Maximum Perfmon Counters Per Session	100
Allowed Cdr Get File Queries Per Minute	10
Allowed Cdr Get File List Queries Per Minute	20
File Close Thread Flag	T
File Close Thread Queue Watermark	100
Restrict On User Group Overlap	1

Enterprise Parameters

Parameter Name	Parameter Value
Restrict Non Super User	T
User Assignment Mode	0
Directory Group Operations On Cisco I Mand Presence	0
Group Size To Limit Presence Packets For Enterprise Groups	100
Syncing Mode For Enterprise Groups	1
Server Port Number	8888
Client Port Number	8889
AA Installed Flag	F
IAQ Installed Flag	F
Organization Domain	
Cluster Name	
Do S Protection Flag	T
TLS Handshake Timer	60
TLS Resumption Timer	3600
Unsupported Pickup	
User Must Change Credential Behavior	
Enable IP V6	F
IP Addressing Mode Pref Media	0
IP Addressing Mode Pref Control	0
Allow Auto Configuration For Phones	1
Allow Duplicate Address Detection	1
Accept Redirect Messages	0
Reply Multicast Echo Request	0
Remote Syslog Server Name	
Remote Syslog Server Name2	
Remote Syslog Server Name3	
Remote Syslog Server Name4	
Remote Syslog Server Name5	
Remote Syslog Severity	3
GRT Socket Connect Timeout	10
GRT Socket Read Timeout	60
Is Logical Partitioning Enabled	F
Is Custom Logical Partitioning Applied	F
Default Geolocation	00000000-1111-0000-0000-000000000000
Logical Partitioning Default Policy	2
Logical Partitioning Default Filter	
Enable Mgcp Trace Log	0
Enable Call Trace Log	1
Max Call Trace Log Files	2000
Call Trace Log File Size	2
Never Start Call With Video	F
DSCP Value	None
Route Plan Report Max Index	1500000
Oauth Token Expiry Timer	60
Refresh Token Expiry Timer	60
Thirdpartyclient_redirecturi	
SSO Login Behavior For Ios	0
O Auth With Refresh Login Flow	0

Enterprise Parameters	
Parameter Name	**Parameter Value**
Use SS Ofor RTMT	1
Enable Directory Partition Search	0
Enable User Search With Customer	1
Max Servers	30
Max Phones	80000
Max Users	160000

3 Presence

The Presence section contains the following items:

- Settings
- Gateways
- Inter-Clustering
- Inter-Domain Federation
- SIP Federation
- XMPP Federation
- Routing
- Settings
- Static Routes
- Method Event-Routing
- Number Expansion
- Domains

3.1 Settings

The Presence > Settings section contains the following items:

- Standard Configuration
- Advanced Configuration

3.1.1 Presence - Standard Configuration

The following settings include global availability sharing capability for all clients that connect to IM and Presence.

Presence Settings	
Name	**Value**
Cluster ID	StandAloneCluster0341f
Enable availability sharing	Y
Allow users to view the availability of other users without being prompted for approval	Y
Enable use of Email Address for Inter-domain Federation	Y
Maximum Contact List Size (per user)	200
Maximum Watchers (per user)	200
CUCM IM and Presence Publish Trunk	SIPTrunkforIMnP
Enable ad-hoc presence subscriptions	Y
Maximum number of ad-hoc subscriptions	50
Ad-hoc subscription time-to-live (seconds)	900
Enable Partitioned Intradomain Federation with LCS/OCS/Lync	Y
Partitioned Intradomain Routing Mode	Basic Routing Mode

3.1.2 Presence - Advanced Configuration

The Advanced Presence Settings include default domain and the IM address scheme. The IM address scheme has two options:

- UserID@[Default Domain]: each user's IM address matches the format UserID@Default_Domain
- Directory URI: each user's IM address matches their Cisco Unified Communications Manager Directory URI setting.

Advanced Presence Settings	
Default Domain	IM Address Scheme
lab.test	UserID@[Default Domain]

3.2 Presence - Gateways

The purpose of a presence gateway is to enable the transfer of presence status information from the configured gateway to the Presence Engine in IM and Presence. The following gateways are supported:

- **Cisco Unified Communications Manager gateway**: You can configure a Cisco Unified Communications Manager server as a presence gateway. The IM and Presence server sends SIP Subscribe messages to Cisco Unified Communications Manager over a SIP trunk (configured on Cisco Unified Communications Manager), which allows the IM and Presence server to receive presence information, for example, phone on/off hook status.
- **Microsoft Exchange (Calendaring) gateway**: You can configure a Microsoft Exchange server (for Microsoft Outlook) as a presence gateway. This allows the IM and Presence server to collect presence information (calendar/meeting status) on a per-user basis and incorporate it into the presence status of the user.

Presence Gateway		
Presence Gateway	Information	
10.5.1.120	Presence Gateway Type	CUCM
	Description	New Presence Gateway

3.3 Presence - Inter-Clustering

You can associate one or more external IM and Presence clusters (peers), which enable you to route requests to user names and phone numbers on other IM and Presence clusters. You can transmit instant messages and presence status across multiple IM and Presence clusters.

Inter-cluster Peer(s)			
Peer Address	AXL Username	Protocol	Users
10.5.1.152	admin	TCP	1

3.4 Inter-Domain Federation

The Inter-Domain Federation section contains the following items:

- SIP Federation
- XMPP Federation

3.4.1 Inter-Domain Federation - SIP Federation

IM and Presence permits integration with a Microsoft OCS foreign domain for interdomain federation. This allows IM and Presence users in an enterprise domain to interact with users of Microsoft Office Communicator in a foreign domain.

Federated Domains			
Domain Name	Description	Integration Type	Direct Federation
microsoft.com	Test SIP Federated Domain	Inter-Domain to OCS/Lync/S4B	N

3.4.2 XMPP Federation

The Extensible Messaging and Presence Protocol (XMPP) is the core protocol on Cisco Unified Presence. This interface provides instant messaging, availability and roster management services. The following objects are defined:

- Settings
- Default Policy
- Exception Policy

3.4.2.1 XMPP Federation - Settings

IM and Presence can be configured for inter-domain federation, that is to dynamically federate with IM and Presence, WebEx, IBM and any XMPP standards-compliant server.

XMPP Federation Settings	
Name	**Value**
XMPP Federation Node Status	Y
Security Mode	TLS Optional
Require client-side security certificates	Y
Enable SASL EXTERNAL on all incoming connections	N
Enable SASL EXTERNAL on all outgoing connections	N

3.4.2.2 XMPP Federation - Default Policy

IM and Presence Service allows you to specify a default policy to either allow or deny all federated traffic from/to all configured federated enterprises. However, you can provision exceptions to this default policy.

XMPP Federation Default Policy	
Default policy for all federated traffic	Allow

3.4.2.3 XMPP Federation - Exception Policy

These are the exceptions to the default XMPP Federation Policy

XMPP Federation Policy Exception	
Domain Name	**Exception Applies To**
*.example.com	All federated packets from/to the above domain/host

3.4.3 Email Federated Domains

Email domains associated with users in the IM and Presence Service deployment. If the IM and Presence Service is configured to use the email address when federating, then all local users are identified by their email address to federated contacts, rather than their IM address. However, if the Enable use of Email Address for Inter-domain Federation parameter is disabled (default setting), then users are identified by their IM address instead, and the email domains listed on this window are not used.

By default, email domains are managed by the system. The system-managed email domains list contains the email domains of all users configured on the system. You can use this window to add email domains in addition to those already managed by the system.

In addition to providing the list of email domains, this window also specifies whether each administrator-managed email domain was configured on the local cluster, peer cluster, or both. Likewise, it also specifies whether each system-managed email domain is in use on the local cluster, peer cluster, or both.

System-managed email domains, by their nature, cannot be edited because they are in use. However, a system-managed email domain automatically becomes an administrator-managed email domain if there are no longer users on the system with that email domain (for example, due to user deletion). You can edit or delete administrator-managed domains.

Email Domains			
Domain Name	**Type**	**Configured/In use on Local Cluster**	**Configured/In use on Peer Cluster(s)**
lab.test	Administrator Managed	N	Y
nd2.com	Administrator Managed	Y	N
lab.test	System Managed	Y	N

3.5 Routing

The Routing section contains the following items:

- Settings

- Static Routes
- Method Event-Routing
- Number Expansion

3.5.1 Routing - Settings

This section contains the proxy server settings for the IM and Presence server.

The Method/Event Routing Status parameter specifies whether the method/event routing module is enabled or disabled in the SIP proxy server.

The Preferred Proxy Listener parameter specifies which SIP proxy listener is considered the preferred listener. The list contains SIP proxy server listeners that you defined in the Transport Listeners window.

Proxy Configuration Settings	
Name	**Value**
CVP Enable ACL Configuration	N
Method/Event Routing Status	On
Preferred Proxy Listener	Default Cisco SIP Proxy TCP Listener

3.5.2 Routing - Static Routes

This section defines static routes that the SIP proxy server uses. A dynamic route represents a path through the network that automatically get calculated according to routing protocols and routing update messages. A static route represents a fixed path through the network that you explicitly configure. Static routes take precedence over dynamic routes.

Method/Event-Based Routing										
Destination Pattern	**Blocked**	**Description**	**Next Hop**	**Next Hop Port**	**Priority**	**Weight**	**Protocol Type**	**Route Type**	**Allow Less-Specific Route**	**In Service**
555.....	N	New Static Route	10.5.1.150	5060	1	1	TCP	User	On	On
666.....	N	A Second Static Route	10.5.1.120	5060	1	1	TCP	User	On	On

3.5.3 Routing - Method Event-Routing

Method-based or event-based routing configure the SIP proxy server to route SIP messages on the basis of their content.

Method/Event-Based Routing						
Name	**Description**	**Content Token**	**Content Category**	**Destination Address**	**Destination Port**	**Protocol Type**
New Method Based Routing Info	For testing	TEST	Method-Based	10.5.1.122	5060	TCP
ProfileConfig	Multi-Login/Change Notification	profileconfig	Event Type-Based	10.5.1.122	5070	TCP
SystemPublish	System Managed Publish	PUBLISH	Method-Based	10.5.1.122	5070	TCP
SystemSubscribe	System Managed Subscribe	SUBSCRIBE	Method-Based	10.5.1.122	5070	TCP

3.5.4 Routing - Number Expansion

Number expansion configuration allows you to provision patterns that expand an extension number to its full E.164 telephone number. You can also use number expansion to strip numbers. You may want to manipulate the telephone number to match global dialing patterns and to route SIP requests accordingly.

Number expansion requires no precedence so ordering is not required. Instead the SIP Proxy processes the rules from the most specific to the least specific.

Number Expansion

Name	Description	Input Pattern	Translation Pattern
NewNumberExpansion	A test	6.....	00336166.....
NewNumberExpansion02	Another test	4.....	00346166.....

3.6 Presence - Domains

By default, domains are managed by the system. The system-managed domains list contains the domains of all users configured on the system. It also specifies whether each system-managed presence domain is in use on the local cluster, peer cluster, or both.

The following domains are managed by the IM and Presence Service:

Presence Domains			
Domain Name	Type	Configured/In use on Local Cluster	Configured/In use on Peer Cluster(s)
newdomain.com	Administrator Managed	Y	N
newdomain2.com	Administrator Managed	Y	N
lab.test	System Managed	Y	N
lab.test	System Managed	N	Y

4 Messaging

The Messaging section contains the following items:

- Settings
- External Server Setup
- External Database
- Third-Party Compliance Server
- External File Servers
- File Transfer
- Compliance
- Group Chat and Persistent Chat
- Group Chat Alias Mapping
- Group Chat System Administrators

4.1 Messaging - Settings

The following settings apply to the global instant messaging (IM) sharing capability for all clients that connect to IM and Presence.

Settings	
Name	Value
Enable instant messaging	Y
Suppress offline instant messaging	N
Allow clients to log instant message history (on supported clients only)	Y
Allow cut & paste in instant messages	Y

4.2 External Server Setup

The External Server Setup section contains the following items:

- External Database
- Third-Party Compliance Server

4.2.1 Messaging - External Databases

External databases are required for:

- To use persistent chat rooms, you must configure a unique external database instance per node.

- If you use an external database for persistent chat logging, consider the size of your database. Archiving all the messages in a chat room is optional, and will increase traffic on the node and consume space on the external database disk. In large deployments, disk space could be quickly consumed. Ensure that your database is large enough to handle the volume of information.

The following external databases are configured:

External Database Settings		
Database Name	**Details**	
mytestdb	Database Type	MSSQL
	Tablespace	-
	Description	a test for IM and P
	User Name	admin
	Hostname	10.5.1.166
	Port Number	1433
	Enable SSL	N
	Certificate Name	< None >

4.2.2 Messaging - Third Party Compliance Servers

To use the third-party compliance solution you must configure a third-party compliance server for each node in the cluster. IM and Presence passes all messages that are sent to or from any users associated with a node to the designated third-party compliance server for that node. The third-party compliance server applies any relevant policy or filtering to the message, and then passes the message back to IM and Presence. IM and Presence delivers the message to the recipient.

The following third-party compliance servers are configured:

Compliance Server Settings		
Name	**Settings**	
newcomplianceserver	Description	For testing
	IP Address	10.5.1.166
	Port	8843

4.2.3 Messaging - External File Servers

Settings for an External File Server on the IM and Presence Service, including the user credentials and the connection information for the External File Server

< No records found >

4.3 Compliance

A compliance server can be used to log and archive all instant messaging traffic. The IM and Presence Service administrator can select which IM, presence, or group chat events are passed to the compliance server(s), and which events are blocked. The events must be selected based on policy.

The IM and Presence IM compliance chapter includes:

- Compliance Settings
- Compliance Profiles
- Compliance Profiles Routing Priority

4.3.1 Compliance - Settings

The following options are available for Instant Message (IM) compliance:

- Not Configured: no compliance solution is used.
- Message Archiver: use built-in Message Archiver component on IM and Presence as the compliance solution and assign a preconfigured external database to one or more nodes.
- Third-Party Compliance Server: use a third-party server as the compliance option.

Compliance Settings

Name	Value
Compliance Server Selection	Message Archiver
Enable Outbound Message Logging	Y
Block message delivery if unable to record in compliance database	Y
Database Assignment	

Node	External Database
10.5.1.122	mytestdb

4.3.2 Compliance - Profiles

A compliance profile contains a set of Jabber Session Manager (JSM) and\or Text Conferencing (TC) events that you can use to monitor for compliance. You can create a compliance profile that consists of only JSM events, only TC events, or a combination of both JSM and TC events.

Within a compliance profile, JSM and TC events are configured which are logged to the compliance server. These events also decide what type of handling is performed by the compliance server, how IM and Presence Service handles error responses from the compliance server, and whether the IM and Presence Service node waits for a response from the compliance server before processing the event further.

Compliance Profile				
Name	**Details**			
NewComplianceProfile	Description	Testing again		
	JSM Events			
		Event	**Packet Type**	**Handling**	**Fire and Forget**
		e_OFFLINE	presence	bounce	N
		e_SERVER	subscription	pass	N
	TC Events			
		Event	**Handling**	**Fire and Forget**
		onClose	bounce	N
SystemDefaultComplianceProfile	Description	Non-modifiable System Default Compliance Profile		
	JSM Events			
		Event	**Packet Type**	**Handling**	**Fire and Forget**
		e_SESSION	all	bounce	N
		es_END	presence	bounce	N
		es_IN	message	bounce	N
		es_OUT	message	bounce	N
	TC Events			
		Event	**Handling**	**Fire and Forget**
		onBeforeInvite	bounce	N
		onBeforeJoin	bounce	N
		onBeforeRoomCreate	bounce	N
		onBeforeSend	bounce	N
		onLeave	bounce	N

4.3.3 Compliance - Routing Priority

Events that are configured in multiple profiles will be routed in the order as specified here.

Compliance Profiles listed by routing priority (top is highest priority):

Compliance Profiles Routing Priority	
Compliance Profiles	**Priority**
SystemDefaultComplianceProfile	0
NewComplianceProfile	1

4.4 Messaging - File Transfer

File Transfer and Managed File Transfer configurations. Assign an External Database and an External File Server on all nodes where Managed File Transfer is to be active. Install the Node Public Key onto each associated External File Server.

The Node Public Key will be invalidated if the node"s assignment is removed. A new Node Public Key will be generated if the node is reassigned.

The Cisco XCP File Transfer Manager service must be active on each node where Managed File Transfer is required.

File Transer	
Name	**Value**
File Transfer Type	PEER2PEER
Maximum File Size (kB)	51200
Managed File Transfer Assignment	**Managed File Transfer Assignment**

Node	**External Database**	**External File Server**
10.5.1.122		

4.5 Messaging - Group Chat and Persistent Chat

This section defines settings to manage the primary chat server alias associated with each node, and configure permanent chat rooms as opposed to temporary (ad-hoc) chat rooms.

Group Chat and Persistent Chat Settings	
Group Chat Alias Settings	
System Automatically Manages Primary Conference Server Aliases	Y
Enable Persistent Chat	
Enable Persistent Chat	Y
Archive all room joins and exits	Y
Archive all room messages	Y
Allow only group chat system administrators to create persistent chat rooms	N
Maximum number of persistent chat rooms allowed	1500
Number of Connections to the Database	5
Database Connection Heartbeat Interval (seconds)	300
Timeout value for persistent chat rooms (minutes)	0
Persistent Chat Database Assignment	**Node** / **External Database**

Node	**External Database**
10.5.1.122	mytestdb

Room Settings	
Room Settings	
Maximum number of rooms allowed	5500
Member Settings	
Rooms are for members only by default	N
Room owners can change whether or not rooms are for members only	Y
Only moderators can invite people to members-only rooms	Y
Room owners can change whether or not only moderators can invite people to members-only rooms	Y
Users can add themselves to rooms as members	N
Room owners can change whether users can add themselves to rooms as members	N
Presence Settings	
Members and administrators who are not in a room are still visible in the room	Y
Room owners can change whether members and administrators who are not in a room are still visible in the room	Y
Rooms are backwards-compatible with older clients	N
Room owners can change whether rooms are backwards-compatible with older clients	Y
Rooms are anonymous by default	Y
Room owners can change whether or not rooms are anonymous	Y
Invite Settings	
Lowest participation level a user can have to invite others to the room	participant

Room owners can change whether members and administrators who are not in a room are still visible in the room	Y
Occupancy Settings	
How many users can be in a room at one time	1000
How many hidden users can be in a room at one time	1000
Default maximum occupancy for a room	50
Room owners can change default maximum occupancy for a room	Y
Chat Message Settings	
Lowest participation level a user can have to send a private message from within the room	visitor
Room owners can change the lowest participation level a user can have to send a private message from within the room	Y
Lowest participation level a user can have to change a room's subject	participant
Room owners can change the lowest participation level a user can have to change a room's subject	Y
Remove all XHTML formatting from messages	Y
Room owners can change XHTML formatting setting	Y
Moderated Room Settings	
Rooms are moderated by default	N
Room owners can change whether rooms are moderated by default	Y
History Settings	
Maximum number of messages that can be retrieved from the archive	100
Number of messages in chat history displayed by default	15
Room owners can change the number of messages displayed in chat history	N

4.6 Messaging - Group Chat Server Aliases

The following additional aliases to a chat server are configured:

Group Chat Server Alias		
Group Chat Server Alias	**Node Name**	**Primary Group**
conference-2-StandAloneCluster0341f.lab.test	10.5.1.122	Y
MyChatServer.lab.test	10.5.1.122	N
MyChatServer2.lab.test	10.5.1.122	N

4.7 Messaging - Group Chat System Administrators

Group chat system administrators can do the following:

- Configure a room
- Join a password-protected room without supplying the password
- Change a room's subject
- Join any room (including members-only rooms)
- Moderate a room
- Join a room when the maximum occupancy is reached
- Destroy a room
- Browse a room for the list of participants
- Query a room and its items
- Remain in a room if the room changes to be members-only, or if their affiliation changes to "none" in a members-only room
- Change the affiliation of other users in a room
- Invite other users to a members-only room (even when members invite is not allowed)

The following Group chat system administrators are configured:

Group Chat System Administrators		
IM Address	**Nickname**	**Description**
Admin@lab.test	ChatAdmin	Group Chat sysadmin

5 Application

The Application section contains the following items:

- Legacy Client Settings
- Settings
- CCMCIP Profile
- Microsoft RCC
- Settings
- User Assignment
- Third-Party Clients
- Third-Party LDAP Servers
- Third-Party LDAP Search Settings
- Client Types

5.1 Application - Settings

The following lists then Cisco Unified Personal Communicator settings that apply to all Cisco Unified Personal Communicator users:

Client Settings	
Name	**Value**
Proxy Listener	Default Cisco SIP Proxy TCP Listener
Primary TFTP Server	10.5.1.120
Backup TFTP Server 1	10.5.1.150
Backup TFTP Server 2	
CSF certificate directory (relative to CSF install directory)	
Directory Server Type	Microsoft Active Directory
Legacy Client LDAP Attribute Mapping	*(see Mappings table below)*

Mappings	
UserID	sAMAccountName
FirstName	givenName
LastName	sn
MiddleName	middleName
Nickname	nickname
Photo	
Title	title
DisplayName	displayName
NamePrefix	namePrefix
NameSuffix	
Gender	gender
BusinessEMail	mail
BusinessPhoneNumber	telephoneNumber
BusinessVoiceMail	
BusinessMobilePhone	mobile
BusinessPager	pager
BusinessFax	facsimileTelephoneNumber
BusinessOtherPhone	otherTelephone
HomeEMail	
HomeMobilePhone	
HomeFax	
URL	url
Organization	Company
PrimaryPhoneNumber	telephoneNumber
AddressStreet	streetAddress
AddressLocation	l
AddressState	st

Client Settings	
Name	**Value**
	AddressPostalCode	postalCode
	AddressCountry	co

5.2 Application - CCMCIP Profile

The folllowing Cisco CallManager Cisco IP Phone (CCMCIP) profiles for Cisco Unified Personal Communicator are configured:

CCMCIP Profile			
Name	**CCMCIP Profile Settings**		**Users in Profile**
CiscoIPPhoneProfile	Description	The Cisco CallManager Cisco IP Phone (CCMCIP) service runs on CUCM and retrieves list of devices of user	bpitt bwayne
	Primary CCMCIP Host	10.5.1.120	
	Backup CCMCIP Host	10.5.1.150	
	Server Certificate Verification	Self Signed or Keystore	
	Is Default CCMCIP Profile	Y	

5.3 Microsoft RCC

The Microsoft RCC section contains the following items:

- Settings
- User Assignment

5.3.1 Microsoft RCC - Settings

This section lists the Computer Telephony Interface (CTI) gateway settings that apply to the CTI gateway. These settings enable call control via TAPI (TSP) to Cisco Unified Communications Manager (CUCM).

Desk Phone Control Settings	
Name	**Value**
Application Status	On
Application Username	admin
Heartbeat Interval (seconds)	8
Session Timer (seconds)	1810
Microsoft Server Type	MOC server OCS/Lync
Cisco Unified Communications Manager Address (1 of 8)	10.5.1.120
Cisco Unified Communications Manager Address (2 of 8)	
Cisco Unified Communications Manager Address (3 of 8)	
Cisco Unified Communications Manager Address (4 of 8)	
Cisco Unified Communications Manager Address (5 of 8)	
Cisco Unified Communications Manager Address (6 of 8)	
Cisco Unified Communications Manager Address (7 of 8)	
Cisco Unified Communications Manager Address (8 of 8)	

5.3.2 Microsoft RCC - User Assignment

IM and Presence can use the Desk Phone Control service. This is not a licensed service, rather, the assignment is needed to limit the users for performance reasons.

Deskphone Control Usage				
User ID	**Last Name**	**Manager**	**Department**	**Assigned Deskphone Control**
bpitt	Pitt		Brad & Pitt Org	N

Deskphone Control Usage				
User ID	**Last Name**	**Manager**	**Department**	**Assigned Deskphone Control**
bwayne	Wayne		Fictional	N

5.4 Third-Party Clients

The Third-Party Clients section contains the following items:

- Third-Party LDAP Servers
- Third-Party LDAP Search Settings

5.4.1 Third-Party Clients - LDAP Servers

Third-Party XMPP clients may wish to provide LDAP based contact search. You can provision LDAP servers on IM and Presence to support LDAP based contact search by third party XMPP clients.

The following LDAP servers to support LDAP based contact search are configured:

LDAP Host Configuration				
Server ID	**Hostname**	**Port**	**Username**	**Enable SSL**
lab.test	10.5.1.166	389	admin	N

5.4.2 Third-Party Clients - LDAP Settings

You must specify the LDAP search settings that will allow IM and Presence to successfully perform contact search for third party XMPP clients.

This references an LDAP server for third-party XMPP client search.

LDAP Search Settings		
Name	**Details**	
LDAP Search Settings	**LDAP Search Settings - Third-Party XMPP Clients**	
	LDAP Server Type	Microsoft Active Directory
	User Object Class	user
	Base Context	DC=lab,DC=test
	User Attribute	SamAccountName
	LDAP Server 1	lab.test
	LDAP Server 2	< None >
	LDAP Server 3	< None >
	Build vCards from LDAP	N
	LDAP attribute to use for vCard FN	
LDAP Attributes	**Searchable LDAP Attributes**	
	Client User Fields	**LDAP User Fields**
	1 first	givenName
	2 last	sn
	3 fullname	cn
	4 email	mail

5.5 Application - Client Type

The IM and Presence service includes a default set of Cisco Unified Communications and third-party client types supported by the client configuration SOAP interface. You should only add a new client type if instructed to do so by a client application. Otherwise, new client types are unsupported and will be removed when you next upgrade IM and Presence.

Enable 'Version Check Required' to verify that users have the minimum version of the software clients installed. If users do not have the minimum version indicated, they will not be able to sign on

The following lists configured Client types:

Client Type			
Type	Minimum Version	Version Check Required	Description
CAD	0.0.0.0	N	Cisco Agent Desktop
CUCC4ST	7.0.0.0	Y	Cisco Phone Control and Presence with IBM Lotus Sametime
CUPC	7.1.0.00000	Y	Cisco Jabber
ClientType	0.0.0.0	N	Report Tests
JABBERANDROID	0.0.0.0	N	Cisco Jabber for Android
JABBERBLACKBERRY	0.0.0.0	N	Cisco Jabber for Blackberry
JABBERCIUS	0.0.0.0	N	Cisco Jabber for Cius
JABBERIPAD	0.0.0.0	N	Cisco Jabber for iPad
JABBERIPHONE	0.0.0.0	N	Cisco Jabber for iPhone
JABBERNOKIA	0.0.0.0	N	Cisco Jabber for Nokia
THIRDAPPSTANDALONE	0.0.0.0	N	Third Party Application Client
THIRDCLIENT	0.0.0.0	N	Third-Party Client
THIRDPARTYAPP	0.0.0.0	N	Third-Party Application