



Parameters Reference Guide for Cisco Jabber 12.5

First Published: 2018-11-29

Last Modified: 2021-03-31

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



Change History

- [New and Changed Information](#), on page iii

New and Changed Information

Parameter Changes

Date	Parameter Name	Description of Change	Section
January, 2021	SSO_Enabled	Removed parameter	<i>Common Policies</i>
April, 2020	ShowCallAlerts	Changed	<i>Client</i>
July, 2019	LogWritingMobile	Changed	<i>Common Policies</i>
November, 2018	OutlookContactResolveMode	Changed - now also supported by Mac.	<i>Presence</i>
	CommonCriteriaEndCallTimeout	New	<i>Common Policies</i>

Other Document Changes

Date	Status	Description	Location
November, 2018	Changed	UC Manager Configuration feature update	Purpose of this Guide
	New	UC Manager Configuration feature	Jabber Client Configuration Methods



CONTENTS

PREFACE

Change History	iii
New and Changed Information	iii

CHAPTER 1

Jabber Overview	1
Purpose of this Guide	1
About Cisco Jabber	1

CHAPTER 2

Jabber Client Configuration	3
Jabber Client Configuration Methods	3
Configuration File Structure	3
XML Structure	4
Example Configuration	4

CHAPTER 3

Client	5
AllowUserSelectChatsFileDirectory	6
AutoAcceptFileTransfer	7
AutoAcceptImage	7
AutosaveChatsLocation	7
CachePasswordMobile	7
CacheSessionCookieInDevice	8
ChatAlert	8
ChatTelephonyEscalationLimit	8
ContactCardonHover	8
DefaultActionOfContactList	9
Disable_IM_History	9
DisableAudioDucking	10

DisableAllMeetingReminder	10
DisableRemoteDesktopControl	10
DisableNonAcceptMeetingReminder	11
DisableStartOnlineForOfflineMeeting	11
EnableAutosave	11
EnableInlineImages	12
EnableFecc	12
EnablePrt	12
EnablePrtEncryption	13
EnableReminderForNoneWebExMeeting	13
ForceLogoutTimerDesktop	13
ForceLogoutTimerMobile	13
Forgot_Password_URL	14
HideCallControlStrip	14
IP_Mode	14
jabber-plugin-config	14
JawsSounds	15
J2JMaxBandwidthKbps	15
MaxNumberOfBookmarks	15
MakeUsernameReadOnly	15
Mention_GroupChat	16
Mention_P2Pchat	16
Mention_PersistentChat	16
MyJabberFilesLocation	17
pChatMeeting	17
pChatShare	17
Persistent_Chat_Enabled	18
Persistent_Chat_Mobile_Enabled	18
PersistentChatTelephonyEnabled	18
PersistIMNotifications	18
PrtCertificateName	19
PRTCertificateUrl	19
PrtLogServerURL	19
RestoreChatOnLogin	19

ScreenReaderShowErrors	20
ShowCallAlerts	20
ShowIconWhenMobile	20
ShowRecentsTab	21
spell_check_enabled	21
spell_check_language	21
STARTUP_AUTHENTICATION_REQUIRED	21
SwapDisplayNameOrder	22
SystemIdleDuringCalls	22
TelephonyOnlyDiscovery	23
UpdateURL	23
LdapAnonymousBinding	23
UseSystemLanguage	24

CHAPTER 4**Options 25**

AdminConfiguredBot	26
AllowUserCustomTabs	26
CalendarAutoRefreshTime	26
CalendarIntegrationType	27
Callhistory_Expire_Days	27
ConfMediaType	27
ConfigRefetchInterval	28
DisableClientConfigExchangeServer	28
DockedWindowPosition	28
DockedWindowVisible	29
Disable_Meeting_SSO_Browser_Cache	29
EnableBridgeConferencing	29
EnableLoadAddressBook	29
EnableCalendarIntegration	30
EnableSaveChatHistoryToExchange	30
EnableVoipSocket	30
ExchangeAuthenticateWithSystemAccount	31
ExchangeAutodiscoverDomain	31
ExchangeDomain	31

Exchange_UseCredentialsFrom 32

ExternalExchangeServer 32

InternalExchangeServer 32

Location_Enabled 33

LOCATION_MATCHING_MODE 33

Location_Mode 33

MacCalendarIntegrationType 33

SaveChatHistoryToExchangeOperationMode 34

Set_Status_Away_On_Inactive 35

Set_Status_Away_On_Lock_OS 35

Set_Status_Inactive_Timeout 35

ShowContactPictures 35

ShowOfflineContacts 35

StartCallWithVideo 36

Start_Client_On_Start_OS 36

UseBridgeForConferenceCalls 36

UserBridgeUriAdmin 37

CHAPTER 5

Phone 39

CcmcipServer1 39

CcmcipServer2 40

CtiServer1 40

CtiServer2 40

E911EdgeLocationWhiteList 40

E911NotificationURL 41

EnableCallPark 41

EnableDSCPPacketMarking 41

EnableE911EdgeLocationPolicy 42

EnableE911OnPremLocationPolicy 42

EnableNGEPolicy 42

LocalAuthenticationWithBiometrics 43

MakeCallHotKey 43

Meeting_Server_Address 43

Meeting_Server_Address_Backup 44

Meeting_Server_Address_Backup2	44
TftpServer1	44
TftpServer2	44
useCUCMGroupForCti	45

CHAPTER 6**On-Premises Policies 47**

DisableMFTForConversationTypes	47
Disallowed_File_Transfer_Types	47
File_Transfer_Enabled	48
PreferredFT	48
Screen_Capture_Enabled	48
ShowScreenCaptureButton	48

CHAPTER 7**Common Policies 51**

AddContactProtocolRateLimit	53
AddContactProtocolTimeLimit	53
AlertOnAvailableEnabled	53
BlockAccessoriesManagerPlugins	54
CiscoTelProtocolCrossLaunchBackNotificationEnabled	54
CiscoTelProtocolCrossLaunchBackSchema	54
ClickToCallProtocolPermissionEnabled	54
ClickToCallWithEditProtocolPermissionEnabled	55
CommonCriteriaEndCallTimeout	55
CTIWindowBehaviour	55
DeskPhoneModeWindowBehavior	56
DetailedLogDurationDesktop	56
DetailedLogDurationMobile	56
Disable_MultiDevice_Message	56
Disallow_File_Transfer_On_Mobile	57
EnableAccessoriesManager	57
EnableBFCPVideoDesktopShare	57
EnableCallPickup	58
EnableCiscoChatProtocol	58
EnableCiscoIMGroupProtocol	58

EnableCiscoIMProtocol	58
EnableCiscoTelConfProtocol	59
EnableCiscoTelProtocol	59
EnableClickToCallProtocol	59
EnableConvertNumberToURI	59
EnableForensicsContactData	60
EnableGroupCallPickup	60
EnableHuntGroup	60
EnableIMProtocol	60
EnableLocalAddressBookSearch	61
EnableLotusNotesContactResolution	61
EnableLotusNotesCLibrarySupport	62
EnableMediaStatistics	62
EnableOtherGroupPickup	62
EnableP2PDesktopShare	63
EnableProfileProtocol	63
EnablePromoteMobile	63
EnableProvisionProtocol	64
EnableSaveChatToFile	64
EnableShareProtocol	64
EnableSingleNumberReach	64
EnableSIPProtocol	65
EnableSIPURIDialling	65
EnableStatusProtocol	65
EnableTelephonyProtocolRateLimit	66
EnableTelProtocol	66
EnableTelProtocolPopupWindow / CiscoTelProtocolPermissionEnabled	66
EnableVideo	66
EnableVoicePush	67
EnableXMPPProtocol	67
ForceC2XDirectoryResolution	67
ForceDevicePin	68
ForceFontSmoothing	68
ForwardVoicemail	68

InitialPhoneSelection	68
InstantMessageLabels	69
LogWritingDesktop	69
LogWritingMobile	70
MuteAudioByDefault	70
Meetings_Enabled	70
PreferP2PDesktopShare	71
PresenceProtocolRateLimit	71
PresenceProtocolTimeLimit	71
PreventDeclineOnHuntCall	71
PrintIMEnabled	72
ProfileProtocolRateLimit	72
ProfileProtocolTimeLimit	72
ProvisionProtocolRateLimit	72
ProvisionProtocolTimeLimit	73
Push_Notification_Enabled	73
Recent_Chats_Enabled	73
RemoteDestinationEditingWithMultipleDevices	73
RememberChatList	74
ScreenShareAuditMessages	74
selfcareURL	74
ServiceDiscoveryExcludedServices	75
ServicesDomainSsoEmailPrompt	75
SharePortRangeSize	75
SharePortRangeStart	76
ShareProtocolRateLimit	76
ShareProtocolTimeLimit	76
ShowSelfCarePortal	76
SoftPhoneModeWindowBehavior	77
TelemetryEnabled	77
TelemetryEnabledOverCellularData	77
TelemetryCustomerID	77
TelephonyProtocolRateLimit	78
TelephonyProtocolTimeLimit	78

Telephony_Enabled 78
 UserDefinedRemoteDestinations 79
 Voicemail_Enabled 79
 VoiceServicesDomain 79
 WhitelistBot 80

CHAPTER 8

Presence 81

DomainsForOutlookPresence 81
 CalendarWebExMeetingPresence 81
 EnableOutlookPresenceIntegration 82
 meetingservice_supportmultimeeting 82
 LoginResource 82
 OutlookContactResolveMode 82
 PresenceServerAddress 83
 PresenceServerURL 83

CHAPTER 9

Voicemail 85

ForwardVoicemail 85
 VoicemailBackup1Server 85
 VoicemailBackup2Server 86
 VoicemailPrimaryServer 86
 VoiceMailService_UseCredentialsFrom 86

CHAPTER 10

Directory Integration 89

Directory Parameters 89
 CDI Parameters 91
 Directory Connection 92
 PrimaryServerName 92
 SecondaryServerName 92
 ServerPort1 92
 ServerPort2 93
 ConnectionUsername 93
 ConnectionPassword 93
 UseSSL 93

UseANR	94
Directory Query	94
BaseFilter	94
GroupBaseFilter	94
PredictiveSearchFilter	94
DisableSecondaryNumberLookups	95
SearchTimeout	95
MinimumCharacterQuery	96
SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5	96
GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5	96
IM Address Scheme	96
UseSipUriToResolveContacts	96
UriPrefix	97
SipUri	97
LdapSupportedMechanisms	97
EnableEmployeeNumber	97
UseLdapReferral	98
LDAP_UseCredentialsFrom	98
LdapUserDomain	99
Contact Photo	99
PhotoUriSubstitutionEnabled	99
PhotoUriSubstitutionToken	99
PhotoUriWithToken	100
PhotoSource	100
PhoneNumberMasks	100
Attribute Mapping Parameters	102
Attributes on the Directory Server	103
UDS Parameters	104
Directory Connection	104
PresenceDomain	104
UdsServer	104
IM Address Scheme	104
UdsPhotoUriWithToken	104

UseSIPURIToResolveContacts	105
UriPrefix	105
SipUri	105
EmailAddress	105
MaxWordsOfFirstName	106
MaxWordsOfLastName	106
Directory Server Configuration Examples	106
Domain Controller Connection	106
KerberosConfiguration	106
Manual Server Connections for Cisco Jabber	107
UDS Integration	108
LDAP Integration with Expressway for Mobile and Remote Access	108
Simple Authentication for Cisco Jabber	109



CHAPTER 1

Jabber Overview

- [Purpose of this Guide, on page 1](#)
- [About Cisco Jabber, on page 1](#)

Purpose of this Guide

The *Cisco Jabber Parameters Reference Guide* includes information to assist you in defining the available parameters for Jabber client configuration.

About Cisco Jabber

Cisco Jabber is a suite of Unified Communications applications that allow seamless interaction with your contacts from anywhere. Cisco Jabber offers IM, presence, audio and video calling, voicemail, and conferencing.

The applications in the Cisco Jabber family of products are:

- Cisco Jabber for Windows
- Cisco Jabber for Mac
- Cisco Jabber for iPhone and iPad
- Cisco Jabber for Android
- Cisco Jabber Softphone for VDI

For more information about the Cisco Jabber suite of products, see <https://www.cisco.com/go/jabber> or <https://www.cisco.com/c/en/us/products/unified-communications/jabber-softphone-for-vdi/index.html>.



CHAPTER 2

Jabber Client Configuration

- [Jabber Client Configuration Methods](#), on page 3
- [Configuration File Structure](#), on page 3
- [Example Configuration](#), on page 4

Jabber Client Configuration Methods

You can configure Jabber client configuration parameters by either:

- using Unified CM Administration interface
- creating the configuration file using an XML editor.

For more information the *Client Configuration Workflow* section of the latest release of the *On-Premises Deployment for Cisco Jabber* or *Cloud and Hybrid Deployments for Cisco Jabber*.

Configuration File Structure

You create client configuration files in an XML format that contains the following elements

XML Declaration

The configuration file must conform to XML standards and contain the following declaration:

```
<?xml version="1.0" encoding="utf-8"?>
```

Root Element

The root element `config`, contains all group elements. You must also add the version attribute to the root element as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
</config>
```

Group Elements

Group elements contain configuration parameters and values. You must nest group elements within the root element.

XML Structure

The following snippet shows the XML structure of a client configuration file:

```
<Client>
  <parameter>value</parameter>
</Client>
<Directory>
  <parameter>value</parameter>
</Directory>
<Options>
  <parameter>value</parameter>
</Options>
<Phone>
  <parameter>value</parameter>
</Phone>
<Policies>
  <parameter>value</parameter>
</Policies>
<Presence>
  <parameter>value</parameter>
</Presence>
<Voicemail>
  <parameter>value</parameter>
</Voicemail>
```

Example Configuration

The following is an example of a configuration file used in an on-premises deployment for all clients:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <PrtLogServerUrl>http://server_name:port/path/prt_script.php</PrtLogServerUrl>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="true" preload="true">
          <tooltip>Cisco</tooltip>
          <icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
          <url>www.cisco.com</url>
        </page>
      </browser-plugin>
    </jabber-plugin-config>
  </Client>
  <Options>
    <Set_Status_Inactive_Timeout>20</Set_Status_Inactive_Timeout>
    <StartCallWithVideo>>false</StartCallWithVideo>
  </Options>
  <Policies>
    <Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>
  </Policies>
  <Directory>
    <PrimaryServerName>dir.example.com</PrimaryServerName>
    <SearchBase1>ou=staff,dc=example,dc=com</SearchBase1>
    <ConnectionUsername>ad_jabber_access@example.com</ConnectionUsername>
    <ConnectionPassword>Jabber</ConnectionPassword>
    <PhotoUriSubstitutionEnabled>True</PhotoUriSubstitutionEnabled>
    <PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>
    <PhotoUriWithToken>http://example.com/phto/sAMAccountName.jpg</PhotoUriWithToken>
  </Directory>
</config>
```



CHAPTER 3

Client

- [AllowUserSelectChatsFileDirectory](#), on page 6
- [AutoAcceptFileTransfer](#), on page 7
- [AutoAcceptImage](#), on page 7
- [AutosaveChatsLocation](#), on page 7
- [CachePasswordMobile](#), on page 7
- [CacheSessionCookieInDevice](#), on page 8
- [ChatAlert](#), on page 8
- [ChatTelephonyEscalationLimit](#), on page 8
- [ContactCardonHover](#), on page 8
- [DefaultActionOfContactList](#), on page 9
- [Disable_IM_History](#), on page 9
- [DisableAudioDucking](#), on page 10
- [DisableAllMeetingReminder](#), on page 10
- [DisableRemoteDesktopControl](#), on page 10
- [DisableNonAcceptMeetingReminder](#), on page 11
- [DisableStartOnlineForOfflineMeeting](#), on page 11
- [EnableAutosave](#), on page 11
- [EnableInlineImages](#), on page 12
- [EnableFecc](#), on page 12
- [EnablePrt](#), on page 12
- [EnablePrtEncryption](#), on page 13
- [EnableReminderForNoneWebExMeeting](#), on page 13
- [ForceLogoutTimerDesktop](#), on page 13
- [ForceLogoutTimerMobile](#), on page 13
- [Forgot_Password_URL](#), on page 14
- [HideCallControlStrip](#), on page 14
- [IP_Mode](#), on page 14
- [jabber-plugin-config](#), on page 14
- [JawsSounds](#), on page 15
- [J2JMaxBandwidthKbps](#), on page 15
- [MaxNumberOfBookmarks](#), on page 15
- [MakeUsernameReadOnly](#), on page 15
- [Mention_GroupChat](#), on page 16

- [Mention_P2Pchat](#), on page 16
- [Mention_PersistentChat](#), on page 16
- [MyJabberFilesLocation](#), on page 17
- [pChatMeeting](#), on page 17
- [pChatShare](#), on page 17
- [Persistent_Chat_Enabled](#), on page 18
- [Persistent_Chat_Mobile_Enabled](#), on page 18
- [PersistentChatTelephonyEnabled](#), on page 18
- [PersistIMNotifications](#), on page 18
- [PrtCertificateName](#), on page 19
- [PRTCertificateUrl](#), on page 19
- [PrtLogServerURL](#), on page 19
- [RestoreChatOnLogin](#), on page 19
- [ScreenReaderShowErrors](#), on page 20
- [ShowCallAlerts](#), on page 20
- [ShowIconWhenMobile](#), on page 20
- [ShowRecentsTab](#), on page 21
- [spell_check_enabled](#), on page 21
- [spell_check_language](#), on page 21
- [STARTUP_AUTHENTICATION_REQUIRED](#), on page 21
- [SwapDisplayNameOrder](#), on page 22
- [SystemIdleDuringCalls](#), on page 22
- [TelephonyOnlyDiscovery](#), on page 23
- [UpdateURL](#), on page 23
- [LdapAnonymousBinding](#), on page 23
- [UseSystemLanguage](#), on page 24

AllowUserSelectChatsFileDirectory

Applies to Cisco Jabber for Windows.

Determines whether users can change the directory for the `MyJabberChats` and `MyJabberFiles` folders.

- `true` (default)—Users can change the directory of the `MyJabberChats` and `MyJabberFiles` folders using the **Change Folder** button on the **Chats** tab of the **Options** dialog.
- `false`—Users are not allowed to change the directory for the `MyJabberChats` and `MyJabberFiles` folders. The **Change Folder** button is not visible on the **Chats** tab of the **Options** dialog. The directory for the `MyJabberChats` and `MyJabberFiles` folders is determined by the `AutosaveChatsLocation` parameter.

If this parameter is not set, then the behavior is as for `true`.

Example: `<AllowUserSelectChatsFileDirectory>true</AllowUserSelectChatsFileDirectory>`

AutoAcceptFileTransfer

Applies to Cisco Jabber desktop clients.

Specifies whether files are automatically accepted by users during file transfer. This parameter doesn't apply to images, which you can configure using the AutoAcceptImage parameter.

- true—Files are automatically accepted to be downloaded when sent in an IM.
- false (default)—Files are not automatically accepted and the recipient must manually agree to receive the file.

Example: `<AutoAcceptFileTransfer>true</AutoAcceptFileTransfer>`

AutoAcceptImage

Applies to Cisco Jabber for desktop clients.

Set up .jpg, .jpeg, .gif, and .png images to be automatically accepted by users. The AutoAcceptFileTransfer parameter (which is off by default) does not affect this parameter as it does not apply to image files.

true (default)—Images are automatically accepted in the client.

false—Images are not automatically accepted and standard file transfer is used.

AutosaveChatsLocation

Applies to Cisco Jabber for Windows.

Defines the path where instant messages and file transfers are automatically saved each time a user closes a conversation. Use the absolute path on the local file system. Chats are saved in a folder called `MyJabberChats` and files are saved in a folder called `MyJabberFiles`.

If the AllowUserSelectChatsFileDirectory parameter is set to false, then this parameter works with the MyJabberFilesLocation parameter as follows:

- If both the AutosaveChatsLocation parameter and the MyJabberFilesLocation parameter have a value, then the MyJabberFilesLocation value takes priority.
- If the MyJabberFilesLocation parameter does not have a value, then the AutosaveChatsLocation value determines the path to the MyJabberChats and MyJabberFiles folders.
- If both the AutosaveChatsLocation parameter and the MyJabberFilesLocation parameter have no value, then all chats and files are saved to the default location (Documents folder).

Example: `<AutosaveChatsLocation>Local_Path</AutosaveChatsLocation>`

CachePasswordMobile

Applies to Cisco Jabber for mobile clients.

Specifies whether the client stores the password in the cache or not.

- true (default)— The client stores the user password in cache; therefore, the users can automatically sign in when the client starts.
- false— The client cannot store the user password in cache; therefore, the users must enter their password each time the client starts.

Example: `<CachePasswordMobile>true</CachePasswordMobile>`

CacheSessionCookieInDevice

Applies to Cisco Jabber for iPhone and iPad

Specifies whether Cisco Jabber for iPhone and iPad should cache the cookies to the iOS keychain. The SSO cookies cached in the iOS keychain allows users to sign in to Cisco Jabber automatically if the app stops working in the background.

- true (default)—The cookies are cached to the iOS keychain.
- false—The cookies are not cached to the iOS keychain.

ChatAlert

Applies to Cisco Jabber for Windows

Specifies the default sound for chat alerts. Users can change this value in the **Sounds and Alerts** tab of the **Options** window.

Example: `<ChatAlert>IMAlert_1</ChatAlert>`

ChatTelephonyEscalationLimit

Applies to Cisco Jabber for Windows.

Defines the maximum number of participants allowed when telephony escalations are enabled for group chats and persistent chat.

Default value is 25 participants. If you set it to zero participants, then the parameter is disabled. However, there is no maximum limit for the participants.

Example: `<ChatTelephonyEscalationLimit>10</ChatTelephonyEscalationLimit>`

ContactCardonHover

Applies to Cisco Jabber for desktop clients.

Specifies whether contact cards are displayed when you hover over contact names in your **Contacts** list and in search result.

- true (default)—The contact card is displayed if you hover over contacts in the hub window or in a search result. For Jabber for Windows the contact card is displayed when you press CTRL + I over a contacts' name.
- false—The contact card is not displayed when you hover over names in the **Contacts** list or in a search result.

Example: `<ContactCardonHover>>false</ContactCardonHover>`

DefaultActionOfContactList

Applies to Cisco Jabber for mobile clients.

Specifies what happens when a Jabber user taps a contact from the contacts list or from the contact search result.

- Chat (default)—The client starts a chat session with the contact.
- Call—The client starts a VoIP call with the contact.



Note These values are case-sensitive.

The setting specified for DefaultActionOfContactList parameter is not applicable for users with a Phone Only or IM Only account. If the **Call** option is configured for users who have full service deployed, then the client starts a mobile call when phone service is not available.

Example: `<DefaultActionOfContactList>Call</DefaultActionOfContactList>`

Disable_IM_History

Applies to all Cisco Jabber clients from 11.8 version onwards.

Specifies whether the client retains the chat history after participants log out. The client retains the chat history until the participants reset Jabber.

If the Disable_IM_History key is false and the participants reopen the chat window, the client displays only the last 200 messages.



Note For persistent chat users, you must use false (default value). If you disable the Disable_IM_History parameter, then it affects the @mention feature in persistent chat rooms.



Note This parameter is not available for IM-only deployments.

- true—Client does not retain the chat history after participants log out.

If the `Disable_IM_History` parameter is true, this takes precedence (the client saves no history) over the following settings:

- **Allow clients to log instant message history** in the IM and Presence Server.
- **Webex Messenger Org Admin > Policy editor > Policy name > Local Archive** option.
- false (default)—Client retains the chat history after participants log out.

To retain chat history, you must also enable either the **Allow clients to log instant message history** option in the IM and Presence Server or the **Webex Messenger Org Admin > Policy editor > Policy name > Local Archive** option in Webex Messenger.

Example: `<Disable_IM_History>true</Disable_IM_History>`

DisableAudioDucking

Applies to Cisco Jabber for Windows

Specifies if the Audio Ducking feature is enabled.

- true—Audio ducking is disabled
- false(default)—Audio ducking is enabled

Example: `<DisableAudioDucking>true</DisableAudioDucking>`

DisableAllMeetingReminder

Applies to Cisco Jabber for Windows and Cisco Jabber for Mac.

Specifies whether users receive reminders for Webex Meetings that are in their Jabber Meetings tab.

- true—Reminders are disabled.
- false (default)—Reminders are enabled.

DisableRemoteDesktopControl

Applies to Cisco Jabber for Windows

Specifies if Remote Desktop Control is enabled within an IM-only share session.

- true—disable Remote Desktop Control
- false(default)—enable Remote Desktop Control

`<DisableRemoteDesktopControl >true</ DisableRemoteDesktopControl >`

DisableNonAcceptMeetingReminder

Applies to Cisco Jabber for desktop clients.

Determines whether the Cisco Jabber popup meeting reminder is displayed for non-accepted Webex Meetings.

- true—The Jabber popup meeting reminder isn't displayed for Webex Meetings that have not been accepted.
- false (default)—The Jabber popup meeting reminder is displayed for non-accepted Webex Meetings.

Example: `<DisableNonAcceptMeetingReminder>>false</DisableNonAcceptMeetingReminder>`

DisableStartOnlineForOfflineMeeting

Applies to Cisco Jabber for Windows

Determines whether the **Start online** button is displayed in the Meetings tab for non-Webex Meetings. This parameter has no effect on Webex Meetings.

- true (default)—The **Start online** button does not display in the Meetings tab for non-Webex Meetings.
- false —The **Start online** button displays in the Meetings tab for non-Webex Meetings.

Example: `<DisableStartOnlineForOfflineMeeting>>false</DisableStartOnlineForOfflineMeeting>`

EnableAutosave

Applies to Cisco Jabber for desktop clients.

Prerequisites:

- Users must have a Cisco Unified Communications Manager account.
- You must also enable local archiving in the Webex (using the Org Admin > Local Archive Policy) or Cisco Unified Communications Manager for IM and Presence (using Messages > Settings > Allow clients to log instant message history) servers.

Specifies whether users can save instant messages to an HTML file automatically, each time they close a conversation. The file persists even the user signs out or resets Jabber.. Enable the option in the client as follows:

- Windows—**File > Options > Chats > Autosave chat session to:**
- Mac—**Jabber > Preferences > Chats > Save chat archives to:**
- true—The check box is available.
- false (default)—The check box is unavailable.

Example: `<EnableAutosave>>true</EnableAutosave>`

Here is an example of the saved HTML file, when the user chooses Documents (default) as the autosave folder, on a Windows platform:

Example:

```
C:\Users\user  
id\Documents\MyJabberChats\userA@domain.com\Chats\userB@domain.com\2019-04-02\userB@domain.com\2019-04-02_10-55-15.html
```

EnableInlineImages

Applies to Cisco Jabber for desktop clients.

Set up inline images so that they are allowed or prevented from being displayed in the client without being downloaded first.

- true (default)—The image is displayed in Jabber automatically.
- false—File transfer is used where users must accept an image to see it.

Example: `<EnableInlineImages>>false</EnableInlineImages>`

EnableFecc

Applies to all Cisco Jabber clients.

Specifies whether the ability to control far-end cameras is enabled in the client.

- true (default)—Far-end camera control is enabled. The **Far-End Camera Control** button is enabled on the call video window.
- false—Far-end camera control is disabled. The **Far-End Camera Control** button is disabled on the call video window, even if the endpoint can control far-end camera.

Example: `<EnableFecc>>false</EnableFecc>`

EnablePrt

Applies to Cisco Jabber for desktop clients.

Specifies if the **Report a problem** menu item is available in the **Help** menu in the client.

- true (default)—The **Report a problem** menu item is available.
- false—The **Report a problem** menu item is removed.

Example: `<EnablePrt>True</EnablePrt>`

If you disable this parameter, users can still manually use the **Start Menu > Cisco Jabber** directory, or the Program files directory and launch the Problem Report Tool manually.

If a user manually creates a PRT, and this parameter value is set to false, then the zip file created from the PRT has no content.

EnablePrtEncryption

Enables problem report encryption. For Cisco Jabber for desktop clients, configure this parameter with the `PRTCertificateName` parameter. For Cisco Jabber for mobile clients, configure this parameter with the `PRTCertificateUrl` parameter.

- `true`—PRT files sent by Cisco Jabber clients are encrypted.
- `false` (default)—PRT files sent by Cisco Jabber clients are not encrypted.

PRT encryption requires a public or private key pair to encrypt and decrypt the Cisco Jabber problem report. For more information, refer to the *Decrypt the Problem Report* section in the document *Features and Options for Cisco Jabber*.

Example: `<EnablePrtEncryption>true</EnablePrtEncryption>`

EnableReminderForNoneWebExMeeting

Applies to Cisco Jabber for Desktop clients.

Specifies whether users receive reminders for Microsoft Outlook, Google Calendar, Mac iCalendar, IBM Notes and other non-Webex Meetings that are in their Jabber Meetings tab.

- `true`—Reminders are enabled.
- `false` (default)—Reminders are disabled.

ForceLogoutTimerDesktop

Applies to Cisco Jabber desktop clients.

Specifies the number of minutes of inactivity before the user is automatically signed out of Cisco Jabber desktop clients. If the parameter is not set, then the client does not sign out automatically.

The value for minutes is from 1 to 480.

Example:

`<ForceLogoutTimerDesktop>15</ForceLogoutTimerDesktop>`

ForceLogoutTimerMobile

Applies to Cisco Jabber mobile clients.

Specifies the number of minutes of inactivity before the user is automatically signed out of Cisco Jabber mobile clients. If the parameter is not set the client does not sign out automatically.

The value for minutes is from 1 to 480.

Example: `<ForceLogoutTimerMobile>15</ForceLogoutTimerMobile>`

Forgot_Password_URL

Applies to Cisco Jabber for Desktop clients.

Specifies the URL of your web page for users to reset or retrieve forgotten passwords.

In hybrid cloud-based deployments, use the Cisco Webex Administration Tool to direct users to the web page to reset or retrieve forgotten passwords.

Example:

```
<Forgot_Password_URL>http://http_servername/Forgot_Password_URL</Forgot_Password_URL>
```

HideCallControlStrip

Applies to Cisco Jabber for Windows.

Specifies whether the call control strip is displayed in the call window.

- **enable**—Displays the call control strip during calls. On the top bar of the Cisco Jabber call window, users have a new option to see or hide the call control strip.
- **disable (default)**—Hides the call control strip during calls. Users see a video-only window without the call control strip.

Example:

```
<HideCallControlStrip>enable</HideCallControlStrip>
```

IP_Mode

Applies to all clients.

Specifies the network IP protocol for the Cisco Jabber client.

- **IPV4_Only**—Jabber will only attempt to make IPv4 connections.
- **IPV6_Only**—Jabber will only attempt to make IPv6 connections.
- **Dual_Stack (Default)**—Jabber can connect with either IPv4 or IPv6.

Example:<IP_Mode>IPV4_Only</IP_Mode>

jabber-plugin-config

Applies to Cisco Jabber for all clients.

Contains plug-in definitions such as custom embedded tabs that display HTML content. For more information, see *Custom Embedded Tab Definitions* section from the document *Features and Options for Cisco Jabber*.

Example:

```
<jabber-plugin-config>
<browser-plugin>
<page refresh="true" preload="true">
<tooltip>Cisco</tooltip>
<icon>http://www.cisco.com/web/fw/i/logo.gif</icon>
<url>www.cisco.com</url>
</page>
</browser-plugin>
</jabber-plugin-config>
```

JawsSounds

Applies to Cisco Jabber for Windows

Determines whether the default Windows notification sound is played when a contact search returns a result.

- true (default)—The default Windows notification sound is played when a contact search returns a result.
- false—No notification sound is played when a contact search returns a result.

J2JMaxBandwidthKbps

Applies to all Cisco Jabber clients in cloud deployments only.

Specifies the maximum bandwidth (in kilobits per second) to be used for Jabber to Jabber calls. The video quality (resolution) of the call is lowered so that it meets the bandwidth limit.

On startup, Cisco Jabber applies this setting from the jabber-config.xml file that is downloaded from Cisco Webex Messenger.

- Minimum value—128 kbps. Values lower than this are automatically increased to 128Kbps.
- Maximum value—4000 kbps. This is the default value. Values higher than 4000 kbps are automatically decreased to 4000 kbps.

MaxNumberOfBookmarks

Applies to Cisco Jabber for desktop and mobile clients.

Specifies the maximum number of bookmarks allowed in persistent chat rooms. The maximum number of bookmarks allowed is 30.

- 30 (default)—sets a maximum of 30 bookmarks.

Example: `<MaxNumberOfBookmarks>30</MaxNumberOfBookmarks>`

MakeUsernameReadOnly

Applies to Cisco Jabber for desktop clients.

Makes the **Username** field on the Sign In screen read-only after the user signs in successfully for the first time.

- true—**Username** field on the Sign In screen becomes read-only after the user signs in successfully for the first time. To enable the **Username** field again, or to switch to a different user, users must reset Cisco Jabber from the File menu.
- false (default)—**Username** field on the Sign In screen remains editable after the user signs in successfully for the first time.

Example: `<MakeUsernameReadOnly>true</MakeUsernameReadOnly>`

Mention_GroupChat

Applies to Cisco Jabber for Windows.

Specifies whether mentions are enabled in group chat.

- true (default)—Enables mentions in group chat.
- false—Disables mentions in group chat.

Example: `<Mention_GroupChat>>false</Mention_GroupChat>`

Mention_P2Pchat

Applies to Cisco Jabber for Windows.

Specifies whether mentions are enabled in person to person chat.

- true (default)—Enables mentions in person to person chat.
- false—Disables mentions in person to person chat.

Example: `<Mention_P2Pchat>>false</Mention_P2Pchat>`

Mention_PersistentChat

Applies to Cisco Jabber for Windows.

Specifies whether mentions are enabled in persistent chat.

- true (default)—Enables mentions in persistent chat.
- false—Disables mentions in persistent chat.

Example: `<Mention_PersistentChat>>false</Mention_PersistentChat>`

MyJabberFilesLocation

Applies to Cisco Jabber for Windows.

Defines the path where instant messages and file transfers are automatically saved each time a user closes a conversation. Chats are saved in a folder called MyJabberChats and files are saved in a folder called MyJabberFiles.

The user sets this parameter in the **Chats** tab of the **Options** dialog. When the user clicks the **Change Folder** button, a browse dialog opens and the filepath to the chosen folder is written to the MyJabberFilesLocation parameter.

This parameter can be set only if the AllowUserSelectChatsFileDirectory parameter is set to false.

This parameter works with the AutosaveChatsLocation parameter as follows:

- If both the AutosaveChatsLocation parameter and the MyJabberFilesLocation parameter have a value, then the MyJabberFilesLocation value takes priority.
- If the MyJabberFilesLocation parameter does not have a value, then the AutosaveChatsLocation value determines the path to the MyJabberChats and MyJabberFiles folders.
- If both the AutosaveChatsLocation parameter and the MyJabberFilesLocation parameter have no value, then all chats and files are saved to the default location (Documents folder).

pChatMeeting

Applies to Cisco Jabber for Windows.

Defines whether the **Meet Now** option is enabled in persistent chat rooms.

- true (default)—Webex Meetings capabilities are enabled for users in persistent chat rooms. Users see the **Meet Now** option displayed.
- false—Webex Meetings capabilities are disabled for users in persistent chat rooms. Users do not see the **Meet Now** option displayed.

Example: `<pChatMeeting>>false</pChatMeeting>`

pChatShare

Applies to Cisco Jabber for Windows.

Defines whether screen sharing capabilities are enabled in persistent chat rooms.

- true (default)—Screen sharing capabilities are enabled for users in persistent chat rooms. Users see the **Share screen** option displayed.
- false—Screen sharing capabilities are disabled for users in persistent chat rooms. Users do not see the **Share screen** option displayed.

Example: `<pChatShare>>false</pChatShare>`

Persistent_Chat_Enabled

Applies to Cisco Jabber for desktop clients.

Specifies whether the persistent chat feature is available in the client.

- true—The persistent chat interface is shown in the client.
- false (default)—The parameter is set to the default value if the setting is not present in the configuration file.

Example: `<Persistent_Chat_Enabled>true</Persistent_Chat_Enabled>`

Persistent_Chat_Mobile_Enabled

Applies to Cisco Jabber for mobile clients.

Specifies if persistent chat is available in the client.

Prerequisites:

You can set the value to true, only if the Cisco Unified Communications Manager Instant Messaging and Presence server version is 11.5su5 or later.

- true—Persistent chat is available in the client. You can set this
- false (default)—Persistent chat is not available in the client.

Example: `<Persistent_Chat_Mobile_Enabled>>false</Persistent_Chat_Mobile_Enabled>`

PersistentChatTelephonyEnabled

Applies to Cisco Jabber for Windows.

Specifies if the **Call** button is available when users are in persistent chat conversations.

- true (default)—Enables the **Call** button in persistent chat, which allows users to click on it to initiate a phone call.
- false—The **Call** button won't be displayed in persistent chat, so users can't initiate a conference.

Example: `<PersistentChatTelephonyEnabled>>false</PersistentChatTelephonyEnabled>`

PersistIMNotifications

Applies to Cisco Jabber for Windows.

Keeps IM notifications of new messages on the screen until you dismiss them so they do not fade away. Newer notifications are stacked above older ones.

- true - Messages can stay on the screen until users dismiss them. Users have the option to turn persistent display off in their **Options** menu under **Notifications**.

- false (default) - Messages do not remain on the screen until dismissed. Messages are displayed and begin to fade away until there is no notification and only a flashing Jabber icon on the taskbar.

PrtCertificateName

Applies to Cisco Jabber for desktop clients.

Specifies the name of a certificate with a public key in the Enterprise Trust or Trusted Root Certificate Authorities certificate store. The certificate public key is used to encrypt Cisco Jabber Problem reports. You must configure this parameter with the EnablePrtEncryption parameter.

Example:<PrtCertificateName>Certificate_Name</PrtCertificateName>

PRTCertificateUrl

Applies to Cisco Jabber for mobile clients.

Specifies the URL to the certificate with a public key in the trusted root certificate store. The client downloads the public key, and uses it to encrypt the Cisco Jabber problem report. If EnablePrtEncryption is true, and no certificate is downloaded, due to a wrong URL or a network problem, Cisco Jabber does not send a PRT.

Example:<PRTCertificateUrl>http://server_name/path/Certificate_Name</PRTCertificateUrl>

PrtLogServerURL

Specifies the custom script for submitting problem reports. For more information, see *Configure Problem Reporting* section from the document *Features and Options for Cisco Jabber*.

Example:<PrtLogServerURL>http://server_name:port/path/prt_script.php</PrtLogServerURL>

RestoreChatOnLogin

Applies to Cisco Jabber for desktop clients.

Specifies if the **Remember my open conversations** check box on the **General** tab of the **Options** window is checked when users first sign in.

- true—The **Remember my open conversations** check box is checked when users sign in to Cisco Jabber for the first time. Each time users sign into the client, Jabber restores all the person-to-person conversations that were open when they signed out.
- false (default)—The **Remember my open conversations** check box isn't checked when users sign in to Cisco Jabber for the first time.

Users can override the initial setting by checking or unchecking the **Remember my open conversations** check box at any time.



Note If chat history isn't enabled, then the restored chat windows are empty.

Example: `<RestoreChatOnLogin>>false</RestoreChatOnLogin>`

ScreenReaderShowErrors

Applies to Cisco Jabber for Windows.

If a screen reader is running, displays informational messages in Jabber as pop-out windows.

- true (default) - If a screen reader is running, messages that are otherwise displayed in the client are instead displayed as pop-out windows for screen readers to capture them. If a screen reader is not running, informational messages are displayed as normal.
- false - If a screen reader is running, messages are not displayed in a pop-out window.

ShowCallAlerts

Applies to all clients

Controls whether the incoming call alerts (toasts) appear.

- true (default)—The alerts appear.
- false—The alerts don't appear.

Example: `<ShowCallAlerts>>false</ShowCallAlerts>`

ShowIconWhenMobile

Applies to Cisco Jabber for mobile clients.

Specifies if the mobile icon is displayed when a user signs in to Jabber using mobile device. The mobile icon is available next to the user's availability status.

The mobile status icon, like other location sharing, is visible only on desktop clients. When ShowIconWhenMobile is enabled, and a user is signed in to both a desktop and mobile client, then only the desktop location is visible.

- On—The mobile icon is displayed. Also, the **Show icon when on mobile** option is not available in the client.
- Off—The mobile icon is not displayed. Also, the **Show icon when on mobile** option is not available in the client.
- Default_on (default)—The mobile icon is displayed only if the user enables **Show icon when on mobile** option in the client. When the user launches the client, by default the **Show icon when on mobile** option is enabled.

- **Default_off**—The mobile icon is displayed only if the user enables **Show icon when on mobile** option in the client. When the user launches the client, by default the **Show icon when on mobile** option is disabled.
- **Empty or no value**—The mobile icon is displayed.

Example:

```
<ShowIconWhenMobile>Default_on</ShowIconWhenMobile>
```

ShowRecentsTab

Applies to Cisco Jabber for Windows.

Specifies if you want to show or hide users' call history in the **Recents** tab on the Cisco Jabber hub window.

- **true (default)**—The **Recents** tab is displayed.
- **false**—The **Recents** tab is not displayed.

Example: `<ShowRecentsTab>false</ShowRecentsTab>`

spell_check_enabled

Applies to Cisco Jabber for Windows.

Specifies whether spell check is enabled in the client. Spell check supports autocorrect, allows users to select the correct word from a list of suggestions, and add a word to the dictionary.

- **true**—Spell check is enabled.
- **false (default)**—Spell check is disabled.

Example: `<spell_check_enabled>true</spell_check_enabled>`

spell_check_language

Applies to Cisco Jabber for Windows.

Specifies the default spell check language used. The client uses the default spell check language set. You can define the default language dictionary that you want the client to use.

From the conversation windows, users can select different default languages for each user they chat with.

Example: `<spell_check_language>1031</spell_check_language>` defines German as the default spell check language.

STARTUP_AUTHENTICATION_REQUIRED

Applies to all the Cisco Jabber clients.

Specifies if Fast Sign-in is enabled for your client or not.

- false (default)—Fast Sign-in is enabled for your client.
- true—Fast Sign-in is disabled for your client.

Prerequisites that are applicable for mobile clients only:

- The `STARTUP_AUTHENTICATION_REQUIRED` parameter has dependency on `CachePasswordMobile` parameter. To enable Fast Sign-in, set `STARTUP_AUTHENTICATION_REQUIRED` to false and `CachePasswordMobile` to true.
- If you have configured `CachePasswordMobile` parameter in releases earlier than 11.8, then in the release 11.9, configure both `STARTUP_AUTHENTICATION_REQUIRED` and `CachePasswordMobile` parameter to enable Fast Sign-in.
- If you have not configured `CachePasswordMobile` parameter in releases earlier than 11.8, then you can configure only `STARTUP_AUTHENTICATION_REQUIRED` parameter to enable Fast Sign-in.

You can configure both of these parameters over Enterprise Mobility Management (EMM) also.

Example:

```
<STARTUP_AUTHENTICATION_REQUIRED>false</STARTUP_AUTHENTICATION_REQUIRED>
```

SwapDisplayNameOrder

Applies to all Cisco Jabber clients.

Specifies that for certain locales, when the **displayname** directory field is empty or not available, users' own display names and the display names of their contacts can be changed to *Lastname, Firstname* format.

- true (default)—In the following locales: Chinese (Hong Kong), Chinese (People's Republic of China), Chinese (Taiwan), Japanese, Korean; the format for users' own display names and the display names of their contacts is in the *Lastname, Firstname* format.
- false—Users' own display names and the display names of their contacts is in the *Firstname, Lastname* format.

Example: `<SwapDisplayNameOrder>false</SwapDisplayNameOrder>`

SystemIdleDuringCalls

Applies to Cisco Jabber for Windows.

Specifies if the screen saver or computer lock function activates during a Cisco Jabber call if the user is inactive, and if the function is enabled on your Windows computer.

This parameter does not control any behavior for incoming calls when the screen is already locked or the screen saver is already on.

- true—Screen saver can activate during calls.

- false (default)—Screen saver cannot activate during calls or when users receive a new incoming call alert. When the call ends, or the new incoming call alert is accepted or rejected, then the screen saver or screen lock is enabled again.

Example: `<SystemIdleDuringCalls>true</SystemIdleDuringCalls>`

TelephonyOnlyDiscovery

Applies to all Cisco Jabber clients operating in on-premises and cloud deployment modes.

You can restrict some Cisco Jabber client users to access phone only services even though your environment is set up for full UC mode.

- True—Cisco Jabber users can access phone services only.
- False (default)—Cisco Jabber users can access all services that you've configured in your environment.

Example:

`<TelephonyOnlyDiscovery>True</TelephonyOnlyDiscovery>`

UpdateURL

Applies to Cisco Jabber desktop clients.

Specifies the URL to the automatic updates XML definition file on your HTTP server. The client uses this URL to retrieve the update XML file. For more information, see *Configure Automatic Updates* section from the document *Features and Options for Cisco Jabber*.

Example: `<UpdateURL>http://http_servername/UpdateURL_file</UpdateURL>`

LdapAnonymousBinding

Applies to all Cisco Jabber clients for on-premises deployments.

Specifies whether or not to bind to the LDAP server using anonymous binding instead of a user or service account.

- true—Cisco Jabber does not use credentials when connecting to the LDAP server. Users are not allowed to enter credentials for the directory service in the **Options** window.
- false (default)—Cisco Jabber uses credentials when connecting to the LDAP server.



Note Do not use the LdapAnonymousBinding parameter with any of the following parameters because they can cause conflicting configuration:

- LDAP_UseCredentialsFrom
- ConnectionUsername and ConnectionPassword

Example: `<LdapAnonymousBinding>true</LdapAnonymousBinding>`

UseSystemLanguage

Applies to Cisco Jabber for Windows Release 11.1(1) onwards.

Specifies which language is used for the client. The language is determined using the following process:

1. The system checks the bootstrap file. If the language is specified in the bootstrap file (using the LANGUAGE parameter), then the specified language is used.
2. If the language is not specified in the bootstrap file, then the system checks the UseSystemLanguage parameter:
 - true—The language is set to the same value as the operating system.
 - false (default)—The client uses the regional language as specified by the user. The regional language is set at **Control Panel > Clock, Language, and Region > Region and Language > Change the date, time, or number format > Formats tab > Format dropdown**.

Example: `<UseSystemLanguage>true</UseSystemLanguage>`

If the language is not specified in the bootstrap file and the UseSystemLanguage parameter is not included in the jabber-config.xml file, then the regional language is used.



Note

When this parameter is specified in the jabber-config.xml file on a TFTP server, it becomes effective only after the client is restarted (**File > Exit**).



CHAPTER 4

Options

- [AdminConfiguredBot](#), on page 26
- [AllowUserCustomTabs](#), on page 26
- [CalendarAutoRefreshTime](#), on page 26
- [CalendarIntegrationType](#), on page 27
- [Callhistory_Expire_Days](#), on page 27
- [ConfMediaType](#), on page 27
- [ConfigRefetchInterval](#), on page 28
- [DisableClientConfigExchangeServer](#), on page 28
- [DockedWindowPosition](#), on page 28
- [DockedWindowVisible](#), on page 29
- [Disable_Meeting_SSO_Browser_Cache](#), on page 29
- [EnableBridgeConferencing](#), on page 29
- [EnableLoadAddressBook](#), on page 29
- [EnableCalendarIntegration](#), on page 30
- [EnableSaveChatHistoryToExchange](#), on page 30
- [EnableVoipSocket](#), on page 30
- [ExchangeAuthenticateWithSystemAccount](#), on page 31
- [ExchangeAutodiscoverDomain](#), on page 31
- [ExchangeDomain](#), on page 31
- [Exchange_UseCredentialsFrom](#), on page 32
- [ExternalExchangeServer](#), on page 32
- [InternalExchangeServer](#), on page 32
- [Location_Enabled](#), on page 33
- [LOCATION_MATCHING_MODE](#), on page 33
- [Location_Mode](#), on page 33
- [MacCalendarIntegrationType](#), on page 33
- [SaveChatHistoryToExchangeOperationMode](#), on page 34
- [Set_Status_Away_On_Inactive](#), on page 35
- [Set_Status_Away_On_Lock_OS](#), on page 35
- [Set_Status_Inactive_Timeout](#), on page 35
- [ShowContactPictures](#), on page 35
- [ShowOfflineContacts](#), on page 35
- [StartCallWithVideo](#), on page 36

- [Start_Client_On_Start_OS](#), on page 36
- [UseBridgeForConferenceCalls](#), on page 36
- [UserBridgeUriAdmin](#), on page 37

AdminConfiguredBot

Applies to Cisco Jabber desktop, iPhone, and iPad clients.

Automatically adds bots to users' contacts list in Jabber, using the Jabber ID assigned to the bot in the company directory. A group **_BotGroup** is created in the users' contacts list. Your users can also add bots manually to their contacts lists.

Example:

```
<AdminConfiguredBot>bot1@example.com;bot2@example.com;bot3@example.com</AdminConfiguredBot>
```

AllowUserCustomTabs

Applies to Cisco Jabber for desktop and mobile clients.

Specifies if users can create custom embedded tabs in the client.

For mobile clients, you can add any number of custom tabs, but only 10 custom tabs appear in the client. If you have added 10 custom tabs in the client, then the users cannot add anymore custom tabs.

- true (default)—Menu option to create custom tabs is shown in the client.
- false— Menu option to create custom tabs is not shown in the client.

Example: `<AllowUserCustomTabs>>false</AllowUserCustomTabs>`

CalendarAutoRefreshTime

Applies to Cisco Jabber for Desktop clients.

Defines the number of minutes after which integrated calendars refresh. The default value is zero, meaning that the calendars do not automatically refresh. This configuration key only works for Google Calendar and IBM Notes calendar integration.

The default value for Mac is five, which means calendars automatically refresh every five seconds. This configuration key only works for Exchange calendar integration.



Note A high frequency refresh may affect performance of the IBM Lotus Notes server.

Example: `<CalendarAutoRefreshTime>0</CalendarAutoRefreshTime>`

CalendarIntegrationType

Applies to Cisco Jabber for Windows.

This parameter works with the Meetings_Enabled parameter.

- 0—Disables calendar integration in the Meetings tab of the client user interface. If you disable this parameter, the Meetings tab in the client is empty, but the Meetings tab remains on the hub window.
- 1—Enables Microsoft Outlook calendar integration in the Meetings tab of the client user interface.
- 2—Enables IBM Lotus Notes calendar integration in the Meetings tab of the client user interface.
- 3—Enables Google Calendar integration in the Meetings tab of the client user interface.

Restart Cisco Jabber to apply the changes.

Example: `<CalendarIntegrationType>1</CalendarIntegrationType>`



Note

- Client users can override this setting on the **Calendar** tab of the **Options** dialog.
- These parameters interact for calendar integration and contact resolution:
 - CalendarIntegrationType
 - EnableLocalAddressBookSearch
 - EnableLotusNotesContactResolution

See the *Feature Configuration for Cisco Jabber* guide for details.

Callhistory_Expire_Days

Applies to all clients.

Specifies the number of days before the call history is deleted. The maximum number of records stored is 250.

If the value is zero or not specified, then the call history will store the maximum number of call records, which is 250.

Example: `<Callhistory_Expire_Days>2</Callhistory_Expire_Days>`

The oldest item is deleted when call history items reach the count 250 or specified expire days.

ConfMediaType

Applies to all clients.

Specifies how the client connects to meetings in Cisco Collaboration Meeting Rooms. For example, if you set the parameter to `WebExOnly`, and when users select `Join` in the Meetings Tab or on the Meeting invitation, they are connected to the conference using Cisco Webex.

Specifies the conference invitation type for Cisco Collaboration Meeting Rooms.

- `BridgeOnly`—The join button joins the conference using SIP.
- `WebExOnly`—The join button joins the conference using Cisco Webex.
- `Nothing defined`—The join button joins the conference using SIP and the link joins the conference using Cisco Webex.

Example: `<ConfMediaType>WebExOnly</ConfMediaType>`

ConfigRefetchInterval

Applies to Cisco Jabber for all clients.

Specifies the interval in hours when Jabber fetches a fresh configuration from the server. Jabber picks a random re-fetch point within an hour before or after the specified value. For example, for a value of 5, Jabber will choose a random time between 4 and 6 hours. Minimum value is 4.

The default value is 8 hours.

Example: `<ConfigRefetchInterval>5</ConfigRefetchInterval>`

DisableClientConfigExchangeServer

Applies to Cisco Jabber for Windows and Cisco Jabber for Mac.

Disables client settings for `InternalExchangeServer` and `ExternalExchangeServer`, and forces to use `InternalExchangeServer` and `ExternalExchangeServer` on TFTP server.

- `true`—Disables client settings for `InternalExchangeServer` and `ExternalExchangeServer`.
- `false` (default)—Enables client settings for `InternalExchangeServer` and `ExternalExchangeServer`

Example:

`<DisableClientConfigExchangeServer>true</DisableClientConfigExchangeServer>`

DockedWindowPosition

Applies to Cisco Jabber for Windows.

Sets the position of the docked window on the user's screen.

- `TopCenter` (default)—The position of the docked window is at the top center of the screen.
- `TopLeft`—The position of the docked window is at the top left of the screen.
- `TopRight`—The position of the docked window is at the top right of the screen.

Example: `<DockedWindowPosition>TopLeft</DockedWindowPosition>`

DockedWindowVisible

Applies to Cisco Jabber for Windows.

Specifies if the docked window displays when the client starts.

- true (default)—The docked window displays when the client starts.
- false—The docked window does not display when the client starts.

Example: `<DockedWindowVisible>>false</DockedWindowVisible>`

Disable_Meeting_SSO_Browser_Cache

Applies to Cisco Jabber for Mac

Specifies the users to enable or disable the browser cache for meeting SSO SessionTicket.

- true—The browser cache is disabled.
- false (default)—The browser cache is enabled.

EnableBridgeConferencing

Applies to all Cisco Jabber clients.

Specifies if the Use my conference service options are available on the client.

- true—Conference service options are shown in the client.
- false(default)—Conference service options are not shown in the client.

Example: `<EnableBridgeConferencing>>true</EnableBridgeConferencing>`

EnableLoadAddressBook

Applies to Cisco Jabber for mobile clients.

Specifies if the native contacts in the phone are loaded on Cisco Jabber contact list or not.

- true(default)—Native contacts are loaded on the Cisco Jabber contact list.
- false—Native contacts are not loaded the Cisco Jabber contact list.

Example: `<EnableLoadAddressBook>>true</EnableLoadAddressBook>`

EnableCalendarIntegration

Applies to Cisco Jabber for mobile clients.

Specifies if the meeting option is available in the client.

- true—The meeting option is available in the client. All events, in the user's device calendar, are integrated with Jabber.
- false (default)—The meeting option is not available in the client.

Example:

```
<EnableCalendarIntegration>true</EnableCalendarIntegration>
```

EnableSaveChatHistoryToExchange

Applies to Cisco Jabber for Windows and Mac for on-premises and Office 365 deployments.

Enables the client to automatically save chat histories to a Cisco Jabber Chats folder in users' Microsoft Outlook application.

- true—Enables saving chat history to an Outlook folder.
- false (default)—Does not save chat history to an Outlook folder.

Example: `<EnableSaveChatHistoryToExchange>true</EnableSaveChatHistoryToExchange>`

EnableVoipSocket

Applies to Cisco Jabber for iPhone and iPad.



Important

We deprecated this parameter as of August 2020 because of changes in Apple Push Notifications (APNs). We have closed the VoIP socket.

Specifies if Jabber uses the VoIP sockets to set up SIP connection with Cisco Unified Communication Manager server. Even if Jabber is inactive, Jabber refreshes the keep alive timer parameter to re-register the Cisco Unified Communication Manager server to keep SIP registered through the VoIP sockets.

If you're using APNs, Jabber users will always receive calls in Jabber even if their Jabber app is inactive. If you're not using APNs, then set this parameter to true to ensure Jabber users receive their calls even if their app is inactive.

Jabber will be registered in the Cisco UC Manager device page until the TCP connection times out by iOS.

- true(default) —VoIP sockets and keep alive timers are enabled to ensure Jabber will receive calls even if it's inactive.
- false—VoIP sockets and keep alive timers are disabled. We recommend you only set the value to false if APNs are enabled. Otherwise, if you set this parameter to false, the SIP connections with Cisco Unified

Communication Manager close after a short period, which is controlled by the operating system, and Jabber becomes inactive.

Cisco Jabber will automatically sign users out if the parameter value is changed.

Example: `<EnableVoipSocket>true</EnableVoipSocket>`

ExchangeAuthenticateWithSystemAccount

Applies to Cisco Jabber for Windows.

An authentication method to the Microsoft Exchange server. To save chat history to a Microsoft Outlook folder, the parameter enables the client to use the operating system account details of the signed-in user to authenticate with the Exchange server. This authentication method uses the Windows NT LAN Manager (NTLM) security protocol.

- **true** (default)—The client uses the operating system account details of the user to authenticate to the Exchange server.
- **false**—The client does not use the user's operating system account details to authenticate to the Exchange server. Instead, users must enter their credentials in the **Outlook** tab of the **Options** dialog.

If you are using an Office 365 deployment, keep the value as false.

Example: `<ExchangeAuthenticateWithSystemAccount>>false</ExchangeAuthenticateWithSystemAccount>`

ExchangeAutodiscoverDomain

Applies to Cisco Jabber for Windows and Mac on-premises deployments.

Specifies the domain that the client uses to search for the Exchange server. This is used when the domain of the exchange server is different to the domain of the users credentials.

Define the value of the parameter as the domain to discover the Exchange server. The client uses the domain to search for the Exchange server at one of the following web addresses:

`https://<domain>/autodiscover/autodiscover.svc`

`https://autodiscover.<domain>/autodiscover/autodiscover.svc`

Example: `<ExchangeAutodiscoverDomain>domain</ExchangeAutodiscoverDomain>`

ExchangeDomain

Applies to Cisco Jabber for desktop clients.

Specifies the domain of the Microsoft Exchange server. This parameter works with the Exchange_UseCredentialsFrom parameter as shown in the following example:

- Exchange_UseCredentialsFrom = CUCM (where the username is in the format username@domain.com)
- ExchangeDomain = otherdomain.com
- In this case, username@otherdomain.com is used to authenticate with the Exchange server.

Use this parameter in the following scenarios:

- If you have different domains for the Exchange Server and Cisco Unified Communications Manager.
- If your Cisco Unified Communications Manager is pre 10.5 Release and you want to authenticate with Office 365. In pre 10.5 Cisco Unified Communications Manager, credentials do not contain a domain, however authentication with Office 365 does require a domain. Use this parameter to set a domain for the Exchange server.



Note For Cisco Jabber for Windows, this parameter does not have any effect if the ExchangeAuthenticateWithSystemAccount parameter is set to true.

Exchange_UseCredentialsFrom

Applies to Cisco Jabber for desktop clients.

An authentication method to the Microsoft Exchange server. To save chat history to a Microsoft Outlook folder, it synchronizes the Exchange credentials using one of the following Authenticator argument credentials for users:

- CUP—Use IM and Presence Service credentials for Exchange
- CUCM—Use Cisco Unified Communications Manager credentials for Exchange
- WEBEX—Use Cisco Webex credentials for Exchange

Example: `<Exchange_UseCredentialsFrom>CUCM</Exchange_UseCredentialsFrom>`.

ExternalExchangeServer

Applies to Cisco Jabber for desktop clients.

Specifies the Exchange server address, the client uses this server when saving chat history to an Outlook folder.

Example: `<ExternalExchangeServer>external_exchange_server</ExternalExchangeServer>`

InternalExchangeServer

Applies to Cisco Jabber for desktop clients.

Method of specifying server address. To save chat history to an Outlook folder, manually defines the internal Exchange server.

Example: `<InternalExchangeServer>Internal_exchange_server</InternalExchangeServer>`

Location_Enabled

Applies to Cisco Jabber for desktop clients.

Applies to Cisco Jabber for Windows.

Specifies whether the Location tab is displayed in Jabber settings or not. The location tab is used for location-related settings.

- true (default)—The Location tab is shown in the client.
- false—The Location tab is not shown in the client.

Example: `<Location_Enabled>>false</Location_Enabled>`

LOCATION_MATCHING_MODE

Applies to Cisco Jabber for desktop clients.

Applies to Cisco Jabber for Windows.

Determines how the client detects the current network locations for the Location feature.

- MacAddressOnly (default)—The client uses the Mac address of the network default gateway.
- MacAddressWithSubnet—The client uses a unique pair of subnet addresses and Mac address of the default gateway.

Example: `<LOCATION_MATCHING_MODE>MacAddressWithSubnet</LOCATION_MATCHING_MODE>`

Location_Mode

Applies to Cisco Jabber for desktop clients.

Applies to Cisco Jabber for Windows.

Specifies whether the Location feature is enabled and whether users are notified when new locations are detected.

- ENABLED (default)—Location feature is turned on. Users are notified when new locations are detected.
- DISABLED—Location feature is turned off. Users are not notified when new locations are detected.
- ENABLEDNOPROMPT—Location feature is turned on. Users are not notified when new locations are detected.

Example: `<Location_Mode>DISABLED</Location_Mode>`

MacCalendarIntegrationType

Applies to Cisco Jabber for Mac.

This parameter works with the Meetings_Enabled parameter to specify which type of calendar to integrate with Jabber.

- 0—Disables calendar integration in the **Meetings** tab of the client. If you disable this parameter, the **Meetings** tab stays in the client but is empty.
- 1— (Default) Enables Microsoft Outlook calendar integration in the **Meetings** tab of the client.
- 2—Enables Mac Calendar integration in the **Meetings** tab of the client.
- 3—Enables Google Calendar integration in the **Meetings** tab of the client.

Example: <MacCalendarIntegrationType>2</MacCalendarIntegrationType>

SaveChatHistoryToExchangeOperationMode

Applies to Cisco Jabber for desktop clients.

Replaces the EnableSaveChatHistoryToExchange parameter.

Specifies if users can save chat history to a Cisco Jabber Chats folder in users' Microsoft Outlook application.

- DisabledByPolicy (default)—Users cannot save chat history to Microsoft Outlook. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is not visible in the client.
- EnabledByPolicy—Chats are saved to Microsoft Outlook. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is visible in the client, but users cannot access it.



Note With this option, you must set up a method of authentication for the client to authenticate with the Exchange server. You can choose to authenticate using single sign-on, or by Syncing credentials. For more information, see the *On-Premises Deployment for Cisco Jabber*.

- DisabledByDefault—Users can save chats to Microsoft Outlook. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is unchecked in the client, but users can change it.
- EnabledByDefault—Users can save chats to Microsoft Outlook. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is checked in the client, but users can change it.
- OnPremOnlyByPolicy—Chats are saved to Microsoft Outlook only when Jabber is on the corporate network. Jabber doesn't save chats to Outlook over MRA. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is visible on the Outlook tab of the Options menu, but it is greyed out and users cannot change it.
- OnPremOnlyByDefault—Users have the option to save chats to Microsoft Outlook only when Jabber is in corporate network. Jabber doesn't save chats to Outlook over MRA. The option **Save chat sessions to "Cisco Jabber Chats" Folder in Microsoft Outlook** is checked on the Outlook tab of the Options menu, but users can change it.

Example:

<SaveChatHistoryToExchangeOperationMode>EnabledByDefault</SaveChatHistoryToExchangeOperationMode>

Set_Status_Away_On_Inactive

Applies to Cisco Jabber for Windows.

Specifies if the availability status changes to **Away** when users are inactive.

- true (default)—Availability status changes to **Away** when users are inactive.
- false—Availability status does not change to **Away** when users are inactive.

Example: `<Set_Status_Away_On_Inactive>>false</Set_Status_Away_On_Inactive>`

Set_Status_Away_On_Lock_OS

Applies to Cisco Jabber for Windows.

Specifies if the availability status changes to **Away** when users lock their operating systems.

- true (default)—Availability status changes to **Away** when users lock their operating systems.
- false—Availability status does not change to **Away** when users lock their operating systems.

Example: `<Set_Status_Away_On_Lock_OS>>false</Set_Status_Away_On_Lock_OS>`

Set_Status_Inactive_Timeout

Applies to Cisco Jabber desktop clients.

Sets the amount of time, in minutes, before the availability status changes to **Away** if users are inactive.

The default value is 15.

Example: `<Set_Status_Inactive_Timeout>10</Set_Status_Inactive_Timeout>`

ShowContactPictures

Applies to Cisco Jabber Windows client.

Specifies if contact pictures display in the contact list.

- true (default)—Contact pictures display in the contact list.
- false—Contact pictures do not display in the contact list.

Example: `<ShowContactPictures>>false</ShowContactPictures>`

ShowOfflineContacts

Applies to Cisco Jabber for Windows and mobile clients only.

Specifies if offline contacts display in the contact list.

- true (default)—Offline contacts display in the contact list.
- false—Offline contacts do not display in the contact list.

Example: `<ShowOfflineContacts>>false</ShowOfflineContacts>`

StartCallWithVideo

Applies to all the Cisco Jabber clients.

Specifies how calls start when users place calls. Calls can start with audio only or audio and video.

- true (default)—Calls always start with audio and video.
- false—Calls always start with audio only.

Example: `<StartCallWithVideo>>false</StartCallWithVideo>`



Important

Server settings take priority over this parameter in the client configuration file. However, if users change the default option in the client user interface, that setting takes priority over both the server and client configurations.

For Cisco Unified Communications Manager release 9.x and later

1. Open the **Cisco Unified CM Administration** interface.
2. Select **System > Enterprise Parameters**.
3. Set a value for the **Never Start Call with Video** parameter and then select **Save**.

Start_Client_On_Start_OS

Applies to Cisco Jabber for Windows.

Specifies if the client starts automatically when the operating system starts.

- true—The client starts automatically.
- false (default)—The client does not start automatically.

Example: `<Start_Client_On_Start_OS>>true</Start_Client_On_Start_OS>`

UseBridgeForConferenceCalls

Applies to all clients.

Specifies if users can use the conference bridge to make conference calls.

- true (default)—Users see **Use My Conference Service** is enabled.

- false—Users see **Use My Conference Service** is disabled.

Example: `<UseBridgeForConferenceCalls>>false</UseBridgeForConferenceCalls>`

UserBridgeUriAdmin

Applies to all clients.

Specifies the pattern for conference service in the client. For example, if the pattern is set as `%%uid%%@example.com`, and the user Adam McKenzie's user id is `amckenzie`, then the conference service is automatically set as `amckenzie@example.com`. This parameter is used with the `EnableBridgeConferencing`.

Example: `<UserBridgeUriAdmin>%%uid%%@example.com</UserBridgeUriAdmin>`



CHAPTER 5

Phone

- [CcmcipServer1](#), on page 39
- [CcmcipServer2](#), on page 40
- [CtiServer1](#), on page 40
- [CtiServer2](#), on page 40
- [E911EdgeLocationWhiteList](#), on page 40
- [E911NotificationURL](#), on page 41
- [EnableCallPark](#), on page 41
- [EnableDSCPPacketMarking](#), on page 41
- [EnableE911EdgeLocationPolicy](#), on page 42
- [EnableE911OnPremLocationPolicy](#), on page 42
- [EnableNGEPolicy](#) , on page 42
- [LocalAuthenticationWithBiometrics](#), on page 43
- [MakeCallHotKey](#), on page 43
- [Meeting_Server_Address](#), on page 43
- [Meeting_Server_Address_Backup](#), on page 44
- [Meeting_Server_Address_Backup2](#), on page 44
- [TftpServer1](#), on page 44
- [TftpServer2](#), on page 44
- [useCUCMGroupForCti](#), on page 45

CcmcipServer1

Applies to all the Cisco Jabber clients.

Specifies the address of the primary CCMCIP server.

This parameter is required:

- Only if the address of your CCMCIP server is not the same as the TFTP server address.

If the address of the CCMCIP server is the same as the TFTP server address, the client can use the TFTP server address to connect to the CCMCIP server.

- In deployments with Cisco Unified Communications Manager Release 8.

In deployments with Cisco Unified Communications Manager release 9 and later, the client can discover the CCMCIP server if you provision the `_cisco-uds` SRV record.

Cisco Unified Communications Manager release 9.x and earlier—If you enable Cisco Extension Mobility, the `Cisco Extension Mobility` service must be activated on the Cisco Unified Communications Manager nodes that are used for CCMCIP. For information about Cisco Extension Mobility, see the *Features and Services* guide for your Cisco Unified Communications Manager release. Example:

```
<CcmcipServer1>server_address</CcmcipServer1>
```

CcmcipServer2

Applies to all the Cisco Jabber clients.

Specifies the address of the secondary CCMCIP server.

Example: `<CcmcipServer2>server_address</CcmcipServer2>`

CtiServer1

Applies to all the Cisco Jabber clients.

Specifies the address of the primary CTI server.

You should specify a CTI server address in the client configuration if users have desk phone devices.

Example: `<CtiServer1>server_address</CtiServer1>`

CtiServer2

Applies to all the Cisco Jabber clients.

Specifies the address of the secondary CTI server.

Example: `<CtiServer2>server_address</CtiServer2>`

E911EdgeLocationWhiteList

Applies to all the Cisco Jabber clients.

Specifies a whitelist of up to 30 Service Set IDs (SSIDs) separated by a semicolon.

You must configure this parameter when the `E911EdgeLocationPolicy` parameter is set to true. Then the client monitors users who connect to the corporate network through Expressway for Mobile and Remote Access network.

Example:

```
<EnableE911EdgeLocationPolicy>true</EnableE911EdgeLocationPolicy>  
<E911EdgeLocationWhiteList>SSID1;SSID2 </E911EdgeLocationWhiteList>
```

E911NotificationURL

Applies to all Cisco Jabber clients.

This feature is available in Full UC mode or Phone Only mode. It's not available to IM Only mode deployment.

Prerequisites: You must have the telephony_enabled parameter set to true.

Displays a customizable disclaimer message or notification to users each time they sign in to Jabber, which they must accept before their telephony capabilities are enabled. This prompt allows users to acknowledge the disclaimer or notification.

Set the value of this parameter to a valid HTML web page URL where you are hosting your notification message.

Example:

```
<E911NotificationURL>http://www.example.com/e911.html</E911NotificationURL>
```

To ensure that the web page renders correctly for all Jabber clients operating outside the corporate network, the web page must be a static HTML page because the scripts and link tags are not supported by the E911NotificationURL parameter.

EnableCallPark

Applies to the Cisco Jabber mobile clients.

Specifies whether the call park feature is available in the client. To access the call park feature, choose the **More** option in the call window.

- true (default)—Call park is enabled.
- false—Call park is disabled. There is no call park option under the **More** button.

Example: `<EnableCallPark>>false</EnableCallPark>`

EnableDSCPpacketMarking

Applies to Cisco Jabber for Mac and Cisco Jabber for mobile clients.

If EnableDSCPpacketMarking is configured with any of these values, then the user will not see **Enable Differentiated Service for Calls** option in the Cisco Jabber client.

Specifies if DSCP marking is applied to the packets:

- true (default)—DSCP marking is enabled and the check box in the client is not shown.
- false—DSCP marking is not made to packets and the check box in the client is not shown.

Example: `<EnableDSCPpacketMarking>>false</EnableDSCPpacketMarking>`

EnableE911EdgeLocationPolicy

Applies to all the Cisco Jabber clients.

Specifies if the client uses the wireless location monitoring service when users connect to the corporate network through Expressway for Mobile and Remote Access.

- true—Cisco Jabber monitors wireless location.

You must also configure the E911EdgeLocationWhiteList parameter with Service Set IDs (SSIDs). You can configure a list of up to 30 SSIDs, separated by a semicolon.

- false (default)—Cisco Jabber doesn't monitor wireless location.

Example:

```
<EnableE911EdgeLocationPolicy>true</EnableE911EdgeLocationPolicy>
<E911EdgeLocationWhiteList>SSID1;SSID2</E911EdgeLocationWhiteList>
```

EnableE911OnPremLocationPolicy

Applies to all the Cisco Jabber clients.

Specifies if the client uses wireless location monitoring service in an on-premises deployment.

- true—Cisco Jabber monitors wireless location.
- false (default)—Cisco Jabber doesn't monitor wireless location.

Example:

```
<EnableE911OnPremLocationPolicy>true</EnableE911OnPremLocationPolicy>
```

EnableNGEPolicy

Applies to all the Cisco Jabber clients.

Specifies if the media is encrypted with the next generation encryption policies, for example AES256-GCM.

You can configure this parameter with one of these 4 values:

- eNever—Media is not encrypted with the next generation encryption policies.
- eOnPremOnly (default)—Media is encrypted with the next generation encryption policies on on-premises network.
- eEdgeOnly—Media is encrypted with the next generation encryption policies on Expressway network.
- eAlways—Media is always encrypted with the next generation encryption policies.

Example: <EnableNGEPolicy>eOnPremOnly</EnableNGEPolicy>

LocalAuthenticationWithBiometrics

Applies to Cisco Jabber for mobile clients.

Specifies if Cisco Jabber uses fingerprint, Touch ID, or Face ID authentication on your users devices to sign in to Jabber.

You can configure this parameter using any of these values:

- **AdminEnabled**—Cisco Jabber prompts your users to authenticate using fingerprint, Touch ID, or Face ID. Users must use biometric authentication to sign into Cisco Jabber or enter their credentials each time they sign in.
- **UserDecision** (default)—Cisco Jabber prompts your users to authenticate using fingerprint, Touch ID, or Face ID. The users can decide if they want to use biometric authentication to sign into Cisco Jabber.
- **AdminDisabled**—Cisco Jabber doesn't use fingerprint, Touch ID, or Face ID authentication. There is no prompt displayed to the user.

If authentication fails, Cisco Jabber prompts your users to enter their credentials each time they sign in.

Example: `<LocalAuthenticationWithBiometrics>AdminDisabled</LocalAuthenticationWithBiometrics>`

MakeCallHotKey

Applies to Cisco Jabber for Windows.

Specifies a key combination to define a keyboard shortcut in the client. The shortcut allows users to copy text from another application and paste it into the client. When you configure a key combination, it overwrites what another application does with that keyboard shortcut.

- **true** (default)—CTRL+SHIFT+J is enabled as the keyboard shortcut to make click-to-call.
- **false**—The keyboard shortcut is disabled.
- **specify your own keyboard shortcut**—Specify another keyboard shortcut as the value for this parameter, for example `MakeCallHotKey=CTRL+SHIFT+R`. Your own defined keyboard shortcut can use the following keys: CTRL and [SHIFT or ALT (but not both)] + a character, or CTRL + a character.

Example: `<MakeCallHotKey>>false</MakeCallHotKey>`

Meeting_Server_Address

Applies to Cisco Jabber desktop clients.

Specifies the primary Cisco Webex Meetings site URL for users.

Cisco Jabber for Windows client populates the meeting site in the user's host account on the **Options** window. Cisco Jabber for Mac client populates the meeting site in the user's host account on the **Preferences > Meetings** window. Users can enter their credentials to set up the host account and access their Webex Meetings, if the meeting site requires credentials.



Important If you specify an invalid meeting site, users cannot add, or edit, any meetings sites in the client user interface.

Example: `<Meeting_Server_Address>Meeting_Site_URL</Meeting_Server_Address>`

Meeting_Server_Address_Backup

Applies to all the Cisco Jabber clients.

Specifies the secondary Cisco Webex Meetings site URL for users.

Example: `<Meeting_Server_Address_Backup>meeting_site_URL</Meeting_Server_Address_Backup>`

Meeting_Server_Address_Backup2

Applies to all the Cisco Jabber clients.

Specifies the tertiary Cisco Webex Meetings site URL for users.

Example: `<Meeting_Server_Address2>meeting_site_URL</Meeting_Server_Address2>`

TftpServer1

Applies to all the Cisco Jabber clients.

Specifies the address of the primary Cisco Unified Communications Manager TFTP service where device configuration files reside. Set one of the following as the value:

- Hostname (*hostname*)
- IP address (*123.45.254.1*)
- FQDN (*hostname.domain.com*)

You should set this parameter in the client configuration only if:

- You deploy the client in phone mode.
- The TFTP server address for the device configuration is different to the TFTP server address for the client configuration.

During installation, you should set the address of the TFTP server where the client configuration file resides with the following argument: TFTP.

Example: `<TftpServer1>hostname</TftpServer1>`

TftpServer2

Applies to all the Cisco Jabber clients.

Specifies the address of the secondary Cisco Unified Communications Manager TFTP service.

Example: `<TftpServer2>hostname</TftpServer2>`

useCUCMGroupForCti

Applies to the Cisco Jabber desktop clients.

Specifies if the Cisco Unified Communications Manager Group handles load balancing for CTI servers. Set one of the following values:

- `true`—The Cisco Unified Communications Manager Group handles CTI load balancing. You should set this value in phone mode deployments only. In full UC mode, the presence server automatically handles CTI load balancing.
- `false` (default)—The Cisco Unified Communications Manager Group does not handle CTI load balancing.

Example: `<useCUCMGroupForCti>true</useCUCMGroupForCti>`



CHAPTER 6

On-Premises Policies

- [DisableMFTForConversationTypes](#), on page 47
- [Disallowed_File_Transfer_Types](#), on page 47
- [File_Transfer_Enabled](#), on page 48
- [PreferredFT](#), on page 48
- [Screen_Capture_Enabled](#), on page 48
- [ShowScreenCaptureButton](#), on page 48

DisableMFTForConversationTypes

Applies to Cisco Jabber for desktop clients.

When the **Managed File Transfer** option is available for the user, use `DisableMFTForConversationTypes` parameter to disable **Managed File Transfer** option for conversation types:

- `P2P`—Managed file transfer is disabled for peer to peer conversations.
- `GroupChat`—Managed file transfer is disabled for group chats.
- `PersistentChat`—Managed file transfer is disabled for persistent chat rooms.

Use a semicolon to delimit multiple conversation types, for example `P2P;GroupChat;PersistentChat`.

Example: `<DisableMFTForConversationTypes>P2P;PersistentChat</DisableMFTForConversationTypes>`

Disallowed_File_Transfer_Types

Applies to all Cisco Jabber clients.

Restricts users from transferring specific file types. You must set the file extensions as the value, for example, `.exe`.

Use a semicolon to delimit multiple file extensions, for example, `.exe;.msi;.rar;.zip`.

Example: `<Disallowed_File_Transfer_Types>.exe;.msi</Disallowed_File_Transfer_Types>`

File_Transfer_Enabled

Applies to all Cisco Jabber clients.

Specifies if users can transfer files to each other using Cisco Jabber client.

- true (default)—Users can transfer files to each other.
- false—Users cannot transfer files to each other.

Example: `<File_Transfer_Enabled>>false</File_Transfer_Enabled>`

PreferredFT

Applies to all the Cisco Jabber clients.

When Cisco Unified Communications Manager IM & Presence server provides both **Managed File Transfer** and **Peer-to-Peer File Transfer**, this parameter specifies the preferred method of transferring files in the Cisco Jabber client.

- MFT—Files are transferred using the managed file transfer option.
- P2P—Files are transferred using peer to peer file transfer.

If the parameter is not defined, the client checks Cisco Unified Communications Manager IM and Presence node, and when managed file transfer is available the client uses this option, otherwise it uses peer to peer file transfer.

Example: `<PreferredFT>P2P</PreferredFT>`

Screen_Capture_Enabled

Applies to Cisco Jabber for desktop clients.

Specifies if users can take screen captures.

- true (default)—Users can take screen captures.
- false—Users cannot take screen captures.

Example: `<Screen_Capture_Enabled>>false</Screen_Capture_Enabled>`

ShowScreenCaptureButton

Applies to Cisco Jabber for Desktop Clients.

Specifies if the Screen capture button is enabled.

- true (default)—Screen capture button is enabled.
- false—Screen capture button is disabled.



Note Disabling this parameter will hide the Screen capture button in Windows and disable it for Mac.

Example: `<ShowScreenCaptureButton>>false</ShowScreenCaptureButton>`



CHAPTER 7

Common Policies

- `AddContactProtocolRateLimit`, on page 53
- `AddContactProtocolTimeLimit`, on page 53
- `AlertOnAvailableEnabled`, on page 53
- `BlockAccessoriesManagerPlugins`, on page 54
- `CiscoTelProtocolCrossLaunchBackNotificationEnabled`, on page 54
- `CiscoTelProtocolCrossLaunchBackSchema`, on page 54
- `ClickToCallProtocolPermissionEnabled`, on page 54
- `ClickToCallWithEditProtocolPermissionEnabled`, on page 55
- `CommonCriteriaEndCallTimeout`, on page 55
- `CTIWindowBehaviour`, on page 55
- `DeskPhoneModeWindowBehavior`, on page 56
- `DetailedLogDurationDesktop`, on page 56
- `DetailedLogDurationMobile`, on page 56
- `Disable_MultiDevice_Message`, on page 56
- `Disallow_File_Transfer_On_Mobile`, on page 57
- `EnableAccessoriesManager`, on page 57
- `EnableBFCPVideoDesktopShare`, on page 57
- `EnableCallPickup`, on page 58
- `EnableCiscoChatProtocol`, on page 58
- `EnableCiscoIMGroupProtocol`, on page 58
- `EnableCiscoIMProtocol`, on page 58
- `EnableCiscoTelConfProtocol`, on page 59
- `EnableCiscoTelProtocol`, on page 59
- `EnableClickToCallProtocol`, on page 59
- `EnableConvertNumberToURI`, on page 59
- `EnableForensicsContactData`, on page 60
- `EnableGroupCallPickup`, on page 60
- `EnableHuntGroup`, on page 60
- `EnableIMProtocol`, on page 60
- `EnableLocalAddressBookSearch`, on page 61
- `EnableLotusNotesContactResolution`, on page 61
- `EnableLotusNotesCLibrarySupport`, on page 62
- `EnableMediaStatistics`, on page 62

- [EnableOtherGroupPickup](#), on page 62
- [EnableP2PDesktopShare](#), on page 63
- [EnableProfileProtocol](#), on page 63
- [EnablePromoteMobile](#), on page 63
- [EnableProvisionProtocol](#), on page 64
- [EnableSaveChatToFile](#), on page 64
- [EnableShareProtocol](#), on page 64
- [EnableSingleNumberReach](#), on page 64
- [EnableSIPProtocol](#), on page 65
- [EnableSIPURIDialling](#), on page 65
- [EnableStatusProtocol](#), on page 65
- [EnableTelephonyProtocolRateLimit](#), on page 66
- [EnableTelProtocol](#), on page 66
- [EnableTelProtocolPopupWindow / CiscoTelProtocolPermissionEnabled](#), on page 66
- [EnableVideo](#), on page 66
- [EnableVoicePush](#), on page 67
- [EnableXMPPProtocol](#), on page 67
- [ForceC2XDirectoryResolution](#), on page 67
- [ForceDevicePin](#), on page 68
- [ForceFontSmoothing](#), on page 68
- [ForwardVoicemail](#), on page 68
- [InitialPhoneSelection](#), on page 68
- [InstantMessageLabels](#), on page 69
- [LogWritingDesktop](#), on page 69
- [LogWritingMobile](#), on page 70
- [MuteAudioByDefault](#), on page 70
- [Meetings_Enabled](#), on page 70
- [PreferP2PDesktopShare](#), on page 71
- [PresenceProtocolRateLimit](#), on page 71
- [PresenceProtocolTimeLimit](#), on page 71
- [PreventDeclineOnHuntCall](#), on page 71
- [PrintIMEnabled](#), on page 72
- [ProfileProtocolRateLimit](#), on page 72
- [ProfileProtocolTimeLimit](#), on page 72
- [ProvisionProtocolRateLimit](#), on page 72
- [ProvisionProtocolTimeLimit](#), on page 73
- [Push_Notification_Enabled](#), on page 73
- [Recent_Chats_Enabled](#), on page 73
- [RemoteDestinationEditingWithMultipleDevices](#), on page 73
- [RememberChatList](#), on page 74
- [ScreenShareAuditMessages](#), on page 74
- [selfcareURL](#), on page 74
- [ServiceDiscoveryExcludedServices](#), on page 75
- [ServicesDomainSsoEmailPrompt](#), on page 75
- [SharePortRangeSize](#), on page 75
- [SharePortRangeStart](#), on page 76

- [ShareProtocolRateLimit](#), on page 76
- [ShareProtocolTimeLimit](#), on page 76
- [ShowSelfCarePortal](#), on page 76
- [SoftPhoneModeWindowBehavior](#), on page 77
- [TelemetryEnabled](#), on page 77
- [TelemetryEnabledOverCellularData](#), on page 77
- [TelemetryCustomerID](#), on page 77
- [TelephonyProtocolRateLimit](#), on page 78
- [TelephonyProtocolTimeLimit](#), on page 78
- [Telephony_Enabled](#), on page 78
- [UserDefinedRemoteDestinations](#), on page 79
- [Voicemail_Enabled](#), on page 79
- [VoiceServicesDomain](#), on page 79
- [WhitelistBot](#), on page 80

AddContactProtocolRateLimit

Applies to Cisco Jabber for Android on Synergy devices.

Specifies the number of times that users can cross-launch after adding a contact with a URL to their contact lists. The Add Contact scheme can be used to add contacts into the contact list of a user with a URL (such as `contact=username@cisco.com`). For example, if the `AddContactProtocolRateLimit` is 3, and the `AddContactProtocolTimeLimit` is 15 seconds, then a user can cross-launch the Add Contact scheme on Cisco Jabber three times every 15 seconds.

You can set the value between 1 to 100. The default value is 3.

Example: `<AddContactProtocolRateLimit>10</AddContactProtocolRateLimit>`

AddContactProtocolTimeLimit

Applies to Cisco Jabber for Android on Synergy devices.

Specifies the time within which users can cross-launch after adding a contact with a URL to their contact lists. You can set the value between 1 to 300 seconds. The default value is 15 seconds.

Examples: `<AddContactProtocolTimeLimit>10</AddContactProtocolTimeLimit>`

AlertOnAvailableEnabled

Applies to Cisco Jabber for desktop clients.

Enables users to add contacts to their availability watch list.

- `true` (default)—Users can add contacts to their availability watch list.
- `false`—Users cannot add contacts to their availability watch list.

Example: `<AlertOnAvailableEnabled>>false</AlertOnAvailableEnabled>`

BlockAccessoriesManagerPlugins

Applies to Cisco Jabber for desktop clients.

Disables specific Accessories Manager plugins from third party vendors such as Jabra or Logitech. You should set the name of the plugin DLL file as the value. Use a comma to separate multiple values.

Example on Microsoft Windows:

```
<BlockAccessoriesManagerPlugins> JabraJabberPlugin.dll,lucpcisco.dll
</BlockAccessoriesManagerPlugins>
```

CiscoTelProtocolCrossLaunchBackNotificationEnabled

Applies to Cisco Jabber for mobile clients.

Specifies if a dialog box is shown asking users whether they want to return to another application when a call ends or to stay in Jabber.

- true (default)—Dialog box is shown.
- false—Dialog box is not shown.

Example:

```
<CiscoTelProtocolCrossLaunchBackNotificationEnabled>>false</CiscoTelProtocolCrossLaunchBackNotificationEnabled>
```

CiscoTelProtocolCrossLaunchBackSchema

Applies to Cisco Jabber for mobile clients.

Users can specify parameters in a URL that are used to launch back to the original app.

CrossLaunchBackSchema is a white list of allowed app schemas that can be cross launched back. You can specify additional parameters with each schema to allow cross launching the app with additional parameters. You can set specific parameters for the launched back schema. For example, for http, you can set the web site “www.cisco.com”. After specifying a schema and any additional parameters, use the semicolon to specify any additional schema you want to add.

- none (default)—No list.
- *schema_names*—Semicolon-delimited list of permitted application types.

Example:

```
<CiscoTelProtocolCrossLaunchBackSchema>AppSchema1://parameter1;
AppSchema2</CiscoTelProtocolCrossLaunchBackSchema>
```

ClickToCallProtocolPermissionEnabled

Applies to Cisco Jabber for Windows.

Specifies if the dialog box is enabled or disabled, which provides information for users to confirm if they want to call using Cisco Jabber, after they click `clicktocall: uri` link.

- true(default)—Dialog box is enabled, and users are asked to confirm if they want to use Cisco Jabber to call.
- false—Dialog box is disabled, and the call is made without requesting confirmation first.

Example: `<ClickToCallProtocolPermissionEnabled>>false</ClickToCallProtocolPermissionEnabled>`

ClickToCallWithEditProtocolPermissionEnabled

Applies to Cisco Jabber for Windows.

Specifies if the dialog box is enabled or disabled, which provides information for users to confirm if they want to use Cisco Jabber to **Call with edit** option, after they click `clicktocall: uri` link.

- true(default)—Dialog box is enabled, and users are asked to confirm that they want to use Cisco Jabber to place the call with edit option.
- false—Dialog box is disabled, and the call is made without requesting confirmation first.

Example:

`<ClickToCallWithEditProtocolPermissionEnabled>>false</ClickToCallWithEditProtocolPermissionEnabled>`

CommonCriteriaEndCallTimeout

Applies to Cisco Jabber for Windows, Cisco Jabber for iPhone and iPad, and Cisco Jabber for Android.

You must already be running Jabber in Common Criteria mode, by deploying the `CC_MODE` installation argument or EMM parameter. When you deploy `CC_MODE`, the `CommonCriteriaEndCallTimeout` parameter is enabled automatically. It ensures that, during an active call, if the user doesn't receive any media data from the other caller for a specific period, then the call is ended automatically. You can change the default value of 300 seconds.

Example: `<CommonCriteriaEndCallTimeout>60</CommonCriteriaEndCallTimeout>`

CTIWindowBehaviour

Applies to Cisco Jabber for Mac.

Specifies the behavior of the conversation window when the user has answered a call in desk phone control mode (CTI mode).

- OnCall (default)—Conversation window is always displayed when a call is answered.
- Never—Conversation window is never displayed when a call is answered.

If you configured this parameter for earlier versions of Cisco Jabber for Windows, it can still be used for this release. However, we recommend using the `DeskPhoneModeWindowBehavior` parameter instead.

Example: `<CTIWindowBehaviour>Never</CTIWindowBehaviour>`

DeskPhoneModeWindowBehavior

Applies to Cisco Jabber for Windows.

Specifies the behavior of the conversation window when the user has answered a call in deskphone control mode (CTI mode).

- OnVideo—Conversation window is only displayed for video calls.
- OnCall (default)—Conversation window is always displayed when a call is answered.
- Never—Conversation window is never displayed when a call is answered.

Example: `<DeskPhoneModeWindowBehavior>Never</DeskPhoneModeWindowBehavior>`

DetailedLogDurationDesktop

Applies to Cisco Jabber for desktop clients.

If you configure the `LogWritingDesktop` parameter with the value `UserCanEnable`, then this parameter defines the number of hours that the desktop client writes logs to the disc. After the defined period expires, all logs are cleared from the disc.

If you do not specify a value for this parameter (default), then the client writes logs to the disc indefinitely, or until the user disables detailed logging.

Example: `<DetailedLogDurationDesktop>10</DetailedLogDurationDesktop>`

DetailedLogDurationMobile

Applies to Cisco Jabber for mobile clients.

If you configure the `LogWritingMobile` parameter with the value `UserCanEnable`, then this parameter defines the number of hours that the mobile client writes logs to the disc. After the defined period expires, all logs are cleared from the disc.

If you do not specify a value for this parameter (default), then the client writes logs to the disc indefinitely, or until the user disables detailed logging.

Example: `<DetailedLogDurationMobile>10<DetailedLogDurationMobile>`

Disable_MultiDevice_Message

Applies to all Cisco Jabber clients in cloud and on-premises deployments.

Disables the multiple device messaging feature.

- true—Disables the multiple device messaging feature.
- false (default)—The multiple device messaging feature is enabled. Users can see all sent and received messages on all devices that they are signed into.



Note Multiple device messaging does not support file transfer or screen captures. Files are available only on the active devices that sent or received the files.

Example:

```
<Disable_MultiDevice_Message>true</Disable_MultiDevice_Message>
```

Disallow_File_Transfer_On_Mobile

Applies to Cisco Jabber for mobile clients.

Specifies whether the user can send or receive files on mobile.

- true—Users cannot send or receive files on mobile.
- false (default)—Users can send or receive files on mobile.

Example: `<Disallow_File_Transfer_On_Mobile>true</Disallow_File_Transfer_On_Mobile>`

EnableAccessoriesManager

Applies to Cisco Jabber for desktop clients.

Enables the accessories API in the client. This API lets accessory vendors create plug-ins to enable call management functionality for devices such as headsets.

- true (default)—Enable the accessories API.
- false—Disable the accessories API.



Note When set to false, call control buttons on some headsets don't work.

Example: `<EnableAccessoriesManager>>false</EnableAccessoriesManager>`

EnableBFCPVideoDesktopShare

Applies to all Cisco Jabber clients.

Enables BFCP video desktop sharing capabilities. For more information, see *Screen Share* chapter from the *Planning Guide for Cisco Jabber*.

- true (default)—Enables BFCP video desktop sharing on the client.
- false—Disables BFCP video desktop sharing.

Example: `<EnableBFCPVideoDesktopShare>>false</EnableBFCPVideoDesktopShare>`

EnableCallPickup

Applies to Cisco Jabber for desktop clients.

Specifies if a user can pickup a call in their call pickup group.

- true—Enables call pickup.
- false (default)—Disables call pickup.

Example: `<EnableCallPickup>true</EnableCallPickup>`

EnableCiscoChatProtocol

Applies to Cisco Jabber for mobile clients.

Specifies if the client registers as the protocol handler for the ciscochat: protocol.

- true (default)—The client registers as the protocol handler for the ciscochat: protocol.
- false—The client does not register as the protocol handler for the ciscochat: protocol.

Example: `<EnableCiscoChatProtocol>>false</EnableCiscoChatProtocol>`

EnableCiscoIMGroupProtocol

Applies to Cisco Jabber for Windows.

Specifies if the client registers as the protocol handler for the ciscoimgroup: URI.

- true (default)—The client registers as the protocol handler for the ciscoimgroup: URI.
- false—The client does not register as the protocol handler for the ciscoimgroup: URI.

Example: `<EnableCiscoIMGroupProtocol>>false</EnableCiscoIMGroupProtocol>`

EnableCiscoIMProtocol

Applies to Cisco Jabber for Android, iPhone and iPad, and Windows.

Specifies if the client registers as the protocol handler for the ciscoim: URI.

- true (default)—The client registers as the protocol handler for the ciscoim: URI.
- false—The client does not register as the protocol handler for the ciscoim: URI.

Example: `<EnableCiscoIMProtocol>>false</EnableCiscoIMProtocol>`

EnableCiscoTelConfProtocol

Applies to Cisco Jabber for Windows.

Specifies if the client registers as the protocol handler for the ciscotelconf: URI.

- true (default)—The client registers as the protocol handler for the ciscotelconf: URI.
- false—The client does not register as the protocol handler for the ciscotelconf: URI.

Example: `<EnableCiscoTelConfProtocol>>false</EnableCiscoTelConfProtocol>`

EnableCiscoTelProtocol

Applies to Cisco Jabber for Android, iPhone and iPad, and Windows.

Specifies if the client registers as the protocol handler for the ciscotel: URI.

- true (default)—The client registers as the protocol handler for the ciscotel: URI.
- false—The client does not register as the protocol handler for the ciscotel: URI.

Example: `<EnableCiscoTelProtocol>>false</EnableCiscoTelProtocol>`

EnableClickToCallProtocol

Applies to Cisco Jabber for Android, iPhone and iPad, and Windows.

Specifies if the client registers as the protocol handler for the clicktocall: URI.

- true (default)—The client registers as the protocol handler for the clicktocall: URI.
- false—The client does not register as the protocol handler for the clicktocall: URI.

Example: `<EnableClickToCallProtocol>>false</EnableClickToCallProtocol>`

EnableConvertNumberToURI

Applies to Cisco Jabber for all clients.

Specifies if Cisco Jabber converts numbers into SIP URI when a user enters numbers in the chat window.

- true(default)—Cisco Jabber converts numbers into SIP URI.
- false—Cisco Jabber doesn't convert numbers into SIP URI.

Example:

`<EnableConvertNumberToURI>>false</EnableConvertNumberToURI>`

EnableForensicsContactData

Applies to Cisco Jabber desktop clients.

Specifies whether users' Contacts folder is collected by the Problem Reporting Tool (PRT) when reporting a problem that is related to their contacts.

- true (default)—Contacts folder is collected by the PRT tool.
- false—Contacts folder is not collected by the PRT tool.

Example: `<EnableForensicsContactData>>false</EnableForensicsContactData>`

EnableGroupCallPickup

Applies to Cisco Jabber for desktop clients.

Applies to Cisco Jabber for Windows.

Specifies if a user can pickup incoming calls in another call pickup group, by entering the call pickup group number.

- true—Enables group call pickup.
- false (default)—Disables group call pickup.

Example: `<EnableGroupCallPickup>>true</EnableGroupCallPickup>`

EnableHuntGroup

Applies to Cisco Jabber for desktop clients.

Specifies if a user can log into a hunt group.

- true—Users can log into their hunt group.
- false (default)—Users cannot log into their hunt group.

Example: `<EnableHuntGroup>>true</EnableHuntGroup>`

EnableIMProtocol

Applies to all Cisco Jabber clients.

Specifies if the client registers as the protocol handler for the im: URI.

- true (default)—The client registers as the protocol handler for the im: URI.
- false—The client does not register as the protocol handler for the im: URI.

Example: `<EnableIMProtocol>>false</EnableIMProtocol>`

EnableLocalAddressBookSearch

Applies to Cisco Jabber for Windows and mobile clients.

Specifies if users can search for local contacts. For Jabber Windows client, users can also add these local contacts to their contact lists.

- true (default)—Users can search for contacts.
- false—Users cannot search for contacts.

For mobile clients (phone only mode), all local contacts will be imported into Jabber contact lists when Jabber starts. You have an option to disable this setting for your users.

Example: `<EnableLocalAddressBookSearch>>false</EnableLocalAddressBookSearch>`



Note These parameters interact for calendar integration and contact resolution:

- CalendarIntegrationType
- EnableLocalAddressBookSearch
- EnableLotusNotesContactResolution

See the *Feature Configuration for Cisco Jabber* guide for details.

EnableLotusNotesContactResolution

Applies to Cisco Jabber for Windows.

Lets users search for and add local IBM Notes contacts to their contact lists.

- true—Users can search for and add local contacts from IBM Notes to their contact lists.



Note The EnableLocalAddressBookSearch parameter must also be set to true.

- false (default)—Users cannot search for or add local contacts from IBM Notes to their contact lists.

Example: `<EnableLotusNotesContactResolution>>true</EnableLotusNotesContactResolution>`



Note These parameters interact for calendar integration and contact resolution:

- CalendarIntegrationType
- EnableLocalAddressBookSearch
- EnableLotusNotesContactResolution

See the *Feature Configuration for Cisco Jabber* guide for details.

EnableLotusNotesCLibrarySupport

Applies to Cisco Jabber for Windows.

Specifies if IBM Lotus Notes is using the C Library.

- true (default)—Notes C Library
- false—Notes C++ Library

Example: `<EnableLotusNotesCLibrarySupport>true</EnableLotusNotesCLibrarySupport>`

EnableMediaStatistics

Applies to all the Cisco Jabber clients.

Allows viewing of real-time audio and video statistics when on a call.

- true (default)—Real-time audio and video statistics can be viewed when on a call.
- false—No real-time audio and video are available when on a call.

Example: `<EnableMediaStatistics>FALSE</EnableMediaStatistics>`

EnableOtherGroupPickup

Applies to Cisco Jabber for desktop clients.

Applies to Cisco Jabber for Windows.

Specifies if a user can pickup an incoming call in a group that is associated with their own call pickup group.

- true—Enables other group call pickup.
- false (default)—Disables other group call pickup.

Example: `<EnableOtherGroupPickup>true</EnableOtherGroupPickup>`

EnableP2PDesktopShare

Applies to Cisco Jabber for Windows.

Allows users to share their screen if they are not on a call.

- true (default)—Allows users to share their screens.
- false—Users cannot do a person to person screen sharing.

Example: `<EnableP2PDesktopShare>>false</EnableP2PDesktopShare>`

EnableProfileProtocol

Applies to Cisco Jabber for mobile clients.

Specifies if the client registers as the protocol handler for the profile: protocol. The profile: protocol shows a contact's Profile screen from other applications.

- true (default)—The client registers as the protocol handler for the profile: protocol.
- false—The client does not register as the protocol handler for the profile: protocol.

Example: `<EnableProfileProtocol>>false</EnableProfileProtocol>`

EnablePromoteMobile

Applies to Cisco Jabber for Windows.

Specifies if the user notification to promote the Cisco Jabber mobile clients is shown in the Cisco Jabber client.

- true —The notification to download the mobile clients is shown in the client.
- false (default)—The notification is not shown.



Note If Cisco Jabber is deployed in Full UC mode, the user will receive this notification only once after it's been enabled. If Cisco Jabber is deployed in a Phone-only mode, the notification will be displayed only if a mobile device has been configured for the user.

You can change the default text of the user notification by configuring the key `PromotionWelcomeText`, the accepted input value is text.

You can also change the download link by configuring the `AndroidDownloadURL` parameter for Android and the `IOSDownloadURL` parameter for iOS. By default these parameters are configured to direct the users to the Cisco Jabber download page on the Google Play Store or the Apple App Store.

Example: `<EnablePromoteMobile>>false</EnablePromoteMobile>`

```
<PromotionWelcomeText> Download the Cisco Jabber for Android app. </PromotionWelcomeText>
```

```
<AndroidDownloadURL> www.example.com/download </AndroidDownloadURL>  
<IOSDownloadURL> www.example.com/download </IOSDownloadURL>
```

EnableProvisionProtocol

Applies to Cisco Jabber for Android, iPhone and iPad, and Mac.

Specifies if the client registers as the protocol handler for URL provisioning.

- true (default)—The client registers as the protocol handler for URL provisioning.
- false—The client does not register as the protocol handler for URL provisioning.

Example: `<EnableProvisionProtocol>>false</EnableProvisionProtocol>`

EnableSaveChatToFile

Applies to Cisco Jabber for desktop clients.

Users must enable local archiving in the Webex (using the Org Admin > Local Archive Policy) or Cisco Unified Communications Manager for IM and Presence (using Messages > Settings > Allow clients to log instant message history) servers.

Allows users to right click on their chats and save them to the file system as HTML.

- true (default)—Users can save their chats to file.
- false—Users cannot save their chats to file.

Example: `<EnableSaveChatToFile>>false</EnableSaveChatToFile>`

EnableShareProtocol

Applies to Cisco Jabber for mobile.

Specifies if the client registers as the protocol handler for the share: URI. The share: URI shares files or messages from other applications with a contact through Cisco Jabber.

- true (default)—The client registers as the protocol handler for the share: URI.
- false—The client does not register as the protocol handler for the share: URI.

Example: `<EnableShareProtocol>>false</EnableShareProtocol>`

EnableSingleNumberReach

Applies to Cisco Jabber for all clients.

Specifies if users can access Single Number Reach option.

Users can access Single Number Reach only when it is configured in Cisco Unified Communications Manager and EnableSingleNumberReach parameter is enabled.

- true (Default)—User can access Single Number Reach option provided it is also configured in Cisco Unified Communications Manager.
- false—User cannot access Single Number Reach option.

Example:

```
<EnableSingleNumberReach>true</EnableSingleNumberReach>
```

EnableSIPProtocol

Applies to all Cisco Jabber clients.

Specifies if the client registers as the protocol handler for the sip: URI.

- true (default)—The client registers as the protocol handler for the sip: URI.
- false—The client does not register as the protocol handler for the sip: URI.

Example: `<EnableSIPProtocol>>false</EnableSIPProtocol>`

EnableSIPURIDialling

Applies to all Cisco Jabber clients.

Enables URI dialing with Cisco Jabber and allows users to make calls with URIs.

- true—Users can make calls with URIs.
- false (default)—Users cannot make calls with URIs.

Example: `<EnableSIPURIDialling>>true</EnableSIPURIDialling>`

EnableStatusProtocol

Applies to Cisco Jabber for mobile clients.

Specifies if the client registers as the protocol handler for status: protocol. The status: protocol shows the Presence or Edit Presence screens from other applications.

- true (default)—The client registers as the protocol handler for the status: protocol.
- false—The client does not register as the protocol handler for the status: protocol.

Example: `<EnableStatusProtocol>>false</EnableStatusProtocol>`

EnableTelephonyProtocolRateLimit

Applies to Cisco Jabber for Mac.

Specifies if there is a limit on the number of times the telephony protocol handler is used in the client.

- true (default)—Rate limiting is enabled for executing the telephony protocol handlers.
- false—Rate limiting is disabled for executing the telephony protocol handlers.

Example: `<EnableTelephonyProtocolRateLimit>>false</EnableTelephonyProtocolRateLimit>`

EnableTelProtocol

Applies to all Cisco Jabber clients.

Specifies if the client registers as the protocol handler for the tel: URI.

- true (default)—The client registers as the protocol handler for the tel: URI.
- false—The client does not register as the protocol handler for the tel: URI.

Example: `<EnableTelProtocol>>false</EnableTelProtocol>`

EnableTelProtocolPopupWindow / CiscoTelProtocolPermissionEnabled

Applies to Cisco Jabber for Windows.

Specifies whether the dialog box is enabled or disabled, which provides information for users to confirm if they want to make a call using Cisco Jabber, after they click `ciscotel:uri` enabled number.

- true (default)—Dialog box is enabled, and users are asked to confirm that they want to place the call.
- false—Dialog box is disabled, and the call is made without requesting confirmation first. This may cause accidental or unwanted calls.



Note

The `CiscoTelProtocolPermissionEnabled` parameter replaces the `EnableTelProtocolPopupWindow` parameter. Both parameters are supported in the client, however the dialog box is disabled if of the either parameter is set to false.

Example: `<CiscoTelProtocolPermissionEnabled>>false</CiscoTelProtocolPermissionEnabled>`

EnableVideo

Enables or disables video capabilities during a Cisco Jabber video call.

- true (default)—Users can make and receive video calls.
- false—Users cannot make or receive video calls.

Example: `<EnableVideo>>false</EnableVideo>`

EnableVoicePush

Applies to Cisco Jabber for iPhone and iPad.

Specifies if Cisco Jabber receives voice and video push notifications whenever there is a call, even if Cisco Jabber is inactive.

The option to set an automatic away timer is not available when push notifications are enabled.

- true (default)—Push notifications are enabled whenever there is a call.
- false—Push notifications are disabled.

Example: `<EnableVoicePush>>true</EnableVoicePush>`

EnableXMPPProtocol

Applies to Cisco Jabber for Android, iPhone and iPad, and Windows.

Specifies if the client registers as the protocol handler for the xmpp: URI.

- true (default)—The client registers as the protocol handler for the xmpp: URI.
- false—The client does not register as the protocol handler for the xmpp: URI.

Example: `<EnableXMPPProtocol>>false</EnableXMPPProtocol>`

ForceC2XDirectoryResolution

Applies to Cisco Jabber for Windows.

Specifies if the client queries the directory to resolve contact information when users perform click-to-x actions.

- true (default)—The client queries the directory when users perform click-to-x actions.
- false—The client does not query the directory for click-to-x actions.



Note This parameter does not take effect when users connect to the corporate network through Expressway for Mobile and Remote Access. In this case, UDS provides contact resolution and the client cannot query the directory.

Example: `<ForceC2XDirectoryResolution>>false</ForceC2XDirectoryResolution>`

ForceDevicePin

Applies to Cisco Jabber for mobile clients.

This parameter specifies that Jabber must be running on secured devices only. Configure ForceDevicePin parameter with these values:

- false(default)—Jabber does not check if the users have secured their devices.
- true—Jabber checks if the users have secured their devices.

Example:

```
<ForceDevicePin>>false</ForceDevicePin>
```

ForceFontSmoothing

Applies to Cisco Jabber for Windows.

Specifies if the client applies anti-aliasing to smooth text.

- true (default)—The client applies anti-aliasing to text.
- false—The operating system applies anti-aliasing to text.

Example: `<ForceFontSmoothing>>false</ForceFontSmoothing>`

ForwardVoicemail

Applies to all Cisco Jabber clients.

Specifies if users can forward their voice messages to other Jabber users.

- true (default)—Users can forward voice messages.
- false—Users cannot forward voice messages.

Example:

```
<ForwardVoicemail>>true</ForwardVoicemail>
```

InitialPhoneSelection

Sets the phone type for users when the client starts for the first time. Users can change their phone type after starting the client for the first time. The client then saves the user preference, and uses it for the next time when the client starts.

- deskphone—Use the desk phone device for calls.
- softphone (default)—Use the software phone (CSF) device for calls.

The client selects devices in the following order:

1. Software phone devices
2. Desk phone devices

If you don't provide users with software phone devices, then the client automatically selects desk phone devices.

Example: `<InitialPhoneSelection>deskphone</InitialPhoneSelection>`



Note This parameter does not apply to Jabber deployed in a Virtual environment.

InstantMessageLabels

Applies to Cisco Jabber for Windows.

Defines a catalog of security labels, such as SECRET and CONFIDENTIAL, that users must apply before they send an instant message. The label appears before each message that is sent. For example, SECRET: *message text*.

You can specify a maximum of 17 labels.

Cisco Jabber uses the XEP-0258 standard to implement security labels. For more information, refer to *XEP-0258: Security Labels in XMPP*.

Cisco Jabber does not control message distribution based on these labels. Any such control requires the use of a third-party product, such as a compliance server, which supports XEP-0258 label headers.

Example for `jabber-config.xml` for security labels:

```
<InstantMessageLabels>
  <item selector="Classified|SECRET">
    <securitylabel xmlns='urn:xmpp: sec-label:0'>
      <displaymarking fgcolor='black' bgcolor='red'>SECRET </displaymarking>
    </securitylabel>
  </item>
  <item...> ... </item>
</InstantMessageLabels>
```

LogWritingDesktop

Applies to Cisco Jabber for desktop clients.

Defines the level of security for PRT logging by specifying whether logs are written to disc for desktop clients.

- Always (default)—Logs are always written to disc at DEBUG level. No option appears in the client **Help** menu.
- UserCanEnable—Allows users to decide whether logs are written to disc or not. Setting this value creates a **Detailed Logging** option in the **Help** menu of the client, where the user can enable or disable detailed logging. If enabled, DEBUG level logging is created, and if disabled, INFO level logging is created.

- **Never**—Logs are never written to disc. INFO level logging is created. When a PRT is manually generated, in-memory logs are flushed to a temporary file that is deleted as soon as the PRT is generated.

Example: `<LogWritingDesktop>UserCanEnable</LogWritingDesktop>`

For INFO level logging, logs are kept in the in-memory buffer only, which is circular.

For DEBUG level logging, the in-memory buffer is flushed to disc when it is full. When resetting Jabber, all logs on disc are wiped.

LogWritingMobile

Applies to Cisco Jabber for mobile clients.

Defines the level of security for PRT logging by specifying whether Jabber writes logs to disc for mobile clients.

- **Always (default)**—Jabber always writes logs to disc at the INFO level. No option appears in the client **Help** menu.
- **UserCanEnable**—Allows you to decide whether to write logs to disc. Setting this value creates a **Detailed Logging** option in the **Help** menu of the client. You can enable or disable detailed logging. If enabled, creates DEBUG level logging, and if disabled, creates INFO level logging.
- **Never**—Jabber never writes logs to disc. This setting creates INFO level logging. When you manually generate a PRT, Jabber flushes in-memory logs to a temporary file and then deletes the file after generating the PRT.

Example: `<LogWritingMobile>UserCanEnable</LogWritingMobile>`

For INFO level logging, Jabber keeps logs in the in-memory buffer only, which is circular.

For DEBUG level logging, Jabber flushes the in-memory buffer to disc when it is full. Resetting Jabber wipes all logs on disc.

MuteAudioByDefault

Applies to all Cisco Jabber clients.

Specifies if the microphone is automatically muted for all Jabber calls.

- **false (default)**—Your users microphone isn't muted for Jabber calls.
- **true**—Your users microphone is muted for Jabber calls.

Example: `<MuteAudioByDefault>true</MuteAudioByDefault>`

Meetings_Enabled

Applies to all the Cisco Jabber clients.

Enables meetings capabilities in the client. Works in conjunction with the `CalendarIntegrationType` parameter (Windows) and the `MacCalendarIntegrationType` parameter (Mac).

- true (default)—Enables meetings capabilities, allowing you to create meetings and get reminders to join meetings.
- false—Disables meetings capabilities.

Example: `<Meetings_Enabled>>false</Meetings_Enabled>`

PreferP2PDesktopShare

Applies to Cisco Jabber desktop clients.

Specifies that the person to person screen sharing is preferred over video sharing.

- true—Person to person screen sharing is preferred.
- false (default)—Video sharing is preferred.

Example: `<PreferP2PDesktopShare>>true</PreferP2PDesktopShare>`

PresenceProtocolRateLimit

Applies to Cisco Jabber for Android on Synergy devices.

Specifies the number of times that the users can launch the Presence or Edit Presence screens from other applications. For example, if the PresenceProtocolRateLimit is three times, and the PresenceProtocolTimeLimit is 15 seconds, then a user can start the launch of Presence or Edit Presence screens from other applications three times every 15 seconds.

You can set the value between 1 to 100. The default value is 3.

Example: `<PresenceProtocolRateLimit>10</PresenceProtocolRateLimit>`

PresenceProtocolTimeLimit

Applies to Cisco Jabber for Android on Synergy devices.

Specifies the time within which users can launch the Presence or Edit Presence screens from other applications. You can set the value between 1 to 300 seconds. The default value is 15 seconds.

Example: `<PresenceProtocolTimeLimit>5</PresenceProtocolTimeLimit>`

PreventDeclineOn HuntCall

Applies to Cisco Jabber for desktop clients.

Specifies if the Decline button is displayed for an incoming call in a hunt group.

- true—Decline button is not displayed for an incoming call in a hunt group.
- false (default)—Decline button is displayed for an incoming call in a hunt group.

Example: `<PreventDeclineOnHuntCall>true</PreventDeclineOnHuntCall>`

PrintIMEnabled

Applies to Cisco Jabber for Windows.

Specifies whether users have the ability to print conversations from the chat window.

- true (default)—Users can print conversations from the chat window by right-clicking and selecting **Print**.
- false—Users cannot print conversations from the chat window. If they right-click inside the window, the **Print** option is not in the menu.

Example: `<PrintIMEnabled>>false</PrintIMEnabled>`

ProfileProtocolRateLimit

Applies to Cisco Jabber for Android on Synergy devices.

Specifies the number of times that users can launch the Profile screen of a contact from other applications. For example, if the ProfileProtocolRateLimit is three times, and the ProfileProtocolTimeLimit is 15 seconds, then a user can start the launch of the Profile screen of a contact from other applications three times every 15 seconds.

You can set the value between 1 to 100. The default value is 3.

Example: `<ProfileProtocolRateLimit>10</ProfileProtocolRateLimit>`

ProfileProtocolTimeLimit

Applies to Cisco Jabber for Android on Synergy devices.

Specifies the time limit for users to launch the Profile screen of a contact from other applications. You can set the value between 1 to 300 seconds. The default value is 15 seconds.

Example: `<ProfileProtocolTimeLimit>10</ProfileProtocolTimeLimit>`

ProvisionProtocolRateLimit

Applies to Cisco Jabber for Android.

Specifies the number of times the URL provision protocol can be initiated.

For example, if the ProvisionProtocolRateLimit is 3 times, and the ProvisionProtocolTimeLimit is 15 seconds, then a user can launch Cisco Jabber with the URL provision three times every 15 seconds.

You can set the value between 1 to 100. The default value is 3.

Example: `<ProvisionProtocolRateLimit>10</ProvisionProtocolRateLimit>`

ProvisionProtocolTimeLimit

Applies to Cisco Jabber for Android.

Specifies the time within which the URL provision protocol can be initiated. You can set the value between 1 to 300 seconds. The default value is 15 seconds.

Example: `<ProvisionProtocolTimeLimit>10</ProvisionProtocolTimeLimit>`

Push_Notification_Enabled

Applies to Cisco Jabber for iPhone and iPad.

Specifies if Cisco Jabber receives push notifications whenever there is a new IM, even if Cisco Jabber is inactive.

The option to set an automatic away timer is not available when push notifications are enabled.

- true (default)—Push notifications are enabled whenever there is a new IM.
- false—Push notifications are disabled.

Example `<Push_Notification_Enabled>>false</Push_Notification_Enabled`

Recent_Chats_Enabled

Applies to Cisco Jabber for Windows.

Determines whether the Chats tab is available on the Hub window. This parameter is not applicable in phone-only deployments.

- true (default)—the Chats tab is shown on the Hub window.
- false—the Chats tab is not shown on the Hub window.

Example: `<Recent_Chats_Enabled>>false</Recent_Chats_Enabled>`

RemoteDestinationEditingWithMultipleDevices

Applies to Cisco Jabber for Windows.

Allows you to determine whether users with multiple devices can edit or add remote destinations. For more information, see *Configure Extend and Connect* chapter from the document *On-Premises Deployment for Cisco Jabber*.

- true (default)—Users with multiple devices can edit or add remote destinations.
- false—Users with multiple devices cannot edit or add remote destinations.

Example:

`<RemoteDestinationEditingWithMultipleDevices>>false</RemoteDestinationEditingWithMultipleDevices>`

RememberChatList

Applies to Cisco Jabber for mobile clients.

Specifies if the user's chat list is saved and restored after relaunching Jabber.

- **on** (default)—If you set the parameter as *on* or if you leave it empty, then the user's chat list is saved and restored after relaunching Jabber. Also, **Save chat list** option is available in the client.
- **off**—User's chat list is not saved, and **Save chat list** option is not available the client.

Example:

```
<RememberChatList>on</RememberChatList>
```

ScreenShareAuditMessages

Applies to Cisco Jabber for Windows

Enables Jabber clients to send information about all user actions to the Presence server for compliance or auditing purposes.



Note If you also have an active compliance server, the Presence server sends the information to compliance server.

- **true**—Jabber sends information to the Presence server about user actions during IM-only screen sharing.
- **false** (default)—Jabber doesn't send any information to the Presence server about user actions during IM-only screen sharing.



Note If you want to enable this feature, ensure that all Jabber clients are running at least release 11.0(1). For clients earlier than 11.0(1), the collected information during IM-only screen sharing is sent to the clients as instant messages.

Example: `<ScreenShareAuditMessages>>true</ScreenShareAuditMessages>`

selfcareURL

Applies to Cisco Jabber desktop clients.

Specifies the fully qualified domain name (FQDN) of Cisco Unified Communications Manager service.

Defines the URL for the Self Care Portal when no default service profile is selected in Cisco Unified Communications Manager.

Example: `<selfcareURL>http://server_name/selfcareURL</selfcareURL>`

ServiceDiscoveryExcludedServices

Applies to all Cisco Jabber clients.

Specifies whether to exclude certain services from Service Discovery.

- WEBEX—When you set this value, the client:
 - Does not perform CAS lookup
 - Looks for `_cisco-uds`, `_cuplogin`, and `_collab-edge`.
- CUCM—When you set this value, the client:
 - Does not look for `_cisco_uds`
 - Looks for `_cuplogin` and `_collab-edge`.

You can specify multiple, comma-separated values to exclude multiple services.

Example: `<ServiceDiscoveryExcludedServices> WEBEX,CUCM </ServiceDiscoveryExcludedServices>`

ServicesDomainSsoEmailPrompt

Applies to all the Cisco Jabber clients.

Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.

- ON—The prompt is shown.
- OFF (default)—The prompt is not shown.

Example: `<ServicesDomainSsoEmailPrompt>ON</ServicesDomainSsoEmailPrompt>`

SharePortRangeSize

Applies to Cisco Jabber for Windows.

Specifies the size of the port range, when used with the `SharePortRangeStart` parameter. The minimum value is 40. The default is 16383. The value when added to the `SharePortRangeStart` parameter cannot exceed 65535.

For more information on port ranges, see the topic on *Ports and Protocols* in the *Planning Guide for Cisco Jabber*.

Example:

```
<Policies>
<SharePortRangeStart>45130</SharePortRangeStart>
<SharePortRangeSize>100</SharePortRangeSize>
</Policies>
```

SharePortRangeStart

Applies to Cisco Jabber for Windows.

This parameter is used with SharePortRangeSize to specify a port range to use when users share their screen from a chat window.

If you do not configure these parameters, then the client uses the default port range for IM screen share, 49152 to 65535. For more information on default port ranges, see the topic on *Ports and Protocols* in the *Cisco Jabber Planning Guide*.

The value you enter specifies the start of the port range. The minimum value is 1024. The value cannot exceed 65535 minus the SharePortRangeSize.

Example:

```
<Policies>
<SharePortRangeStart>45130</SharePortRangeStart>
<SharePortRangeSize>100</SharePortRangeSize>
</Policies>
```

This example gives the port range 45130 to 45230.

ShareProtocolRateLimit

Applies to Cisco Jabber for Android.

Specifies the number of times sharing files or messages can be initiated. For example, if theShareProtocolRateLimit is 3, and the ShareProtocolTimeLimit is 15 seconds, then a user can start files sharing or message sharing on Cisco Jabber three times every 15 seconds.

You can set the value between 1 to 100. The default value is 3.

Example: <ShareProtocolRateLimit>10</ShareProtocolRateLimit>

ShareProtocolTimeLimit

Applies to Cisco Jabber for Android.

Specifies the time within which sharing files or messages can be initiated. You can set the value between 1 to 300 seconds. The default value is 15 seconds.

Example: <ShareProtocolTimeLimit>10</ShareProtocolTimeLimit>

ShowSelfCarePortal

Applies to Cisco Jabber for desktop clients.

Determines whether the Self Care Portal tab displays in the **Options** dialog.

- true (default)—the Self Care Portal tab displays in the **Options** dialog.
- false—the Self Care Portal tab does not display in the **Options** dialog

Example: `<ShowSelfCarePortal>>false</ShowSelfCarePortal>`

SoftPhoneModeWindowBehavior

Applies to Cisco Jabber for Windows.

Specifies the behavior of the conversation window when the user has answered a call in softphone control mode.

- OnVideo—Conversation window is only displayed for video calls.
- OnCall (default)—Conversation window is always displayed when a call is answered.
- Never—Conversation window is never displayed when a call is answered.

Example: `<SoftPhoneModeWindowBehavior>Never</SoftPhoneModeWindowBehavior>`

TelemetryEnabled

Applies to all Cisco Jabber clients.

Specifies whether Cisco Jabber client gathers the analytics data or not. To improve user experience and product performance, Cisco Jabber client might gather analytics data.

- true (default)—Analytics data will be gathered.
- false—Analytics data will not be gathered.

Example: `<TelemetryEnabled>>false</TelemetryEnabled>`

TelemetryEnabledOverCellularData

Applies to Cisco Jabber for mobile clients.

Specifies whether analytics data will be sent over Wi-Fi.

- true (default)—Analytics data will be sent over Wi-Fi and mobile data connections.
- false—Analytics data will be sent over Wi-Fi connections only.

Example: `<TelemetryEnabledOverCellularData>>false</TelemetryEnabledOverCellularData>`

TelemetryCustomerID

Applies to all the Cisco Jabber clients.

Specifies the source of analytic information. This can be a string that explicitly identifies an individual customer or a string that identifies a common source without identifying the customer. Cisco recommends using a Global Unique Identifier (GUID) generating utility to generate a 36 character unique identifier or to use a reverse domain name. The following utilities are available for generating a GUID:

- Mac OS X - uuidgen
- Linux - uuidgen
- Microsoft Windows - [guid]::NewGuid().ToString() or (from cmd.exe) powershell -command "[guid]::NewGuid().ToString()"
- Online - guid.us

This identifier must be globally unique regardless of the method used to create the GUID.

Example: `<TelemetryCustomerID>customerIdentifier</TelemetryCustomerID>`

TelephonyProtocolRateLimit

Applies to Cisco Jabber for Windows, Mac, and Android.

Specifies the number of times a call can be initiated from one of the telephony protocol handlers (tel: ciscotel, sip). For example, if the TelephonyProtocolRateLimit is 2, and the TelephonyProtocolTimeLimit is 10 seconds, then a user can start a call from one of the telephony protocol handlers two times every 10 seconds.

You can set the value between 1 to 100. The default value is 2.



Note Only one protocol handler can be processed at one time. Any other protocol handler arriving when the user already has a call alert are either discarded or queued up.

Example: `<TelephonyProtocolRateLimit>10</TelephonyProtocolRateLimit>`

TelephonyProtocolTimeLimit

Applies to Cisco Jabber for Windows, Mac, and Android.

Specifies the time within which a user can start a call from one of the telephony protocol handlers (sip, tel, ciscotel) before the TelephonyProtocolRateLimit is hit or reset. The default value for initiating a call from one of the telephony protocol handlers is 10 seconds for every two attempts. You can set the value between 1-300 seconds.

Example: `<TelephonyProtocolTimeLimit>10</TelephonyProtocolTimeLimit>`

Telephony_Enabled

Applies to all Cisco Jabber clients.

Enables audio and video capabilities and user interface in the client.

- true (default)—Enables audio and video capabilities and user interface.
- false—Disables audio and video capabilities and user interface.

If your client is enabled for IM-only mode, then you must set this parameter to false. If you do not set this parameter in IM-only mode deployments, then users may see disabled telephony capabilities on their user interface.

Example: `<Telephony_Enabled>>false</Telephony_Enabled>`

UserDefinedRemoteDestinations

Applies to Cisco Jabber for Windows.

Lets users add, edit, and delete remote destinations through the client interface. Use this parameter to change the default behavior when you provision Extend and Connect capabilities.

By default, if a user's device list contains only a CTI remote device, the client does not let that user add, edit, or delete remote destinations. This occurs to prevent users from modifying dedicated remote devices that you assign. However, if the user's device list contains a software device or a desk phone device, the client lets users add, edit, and delete remote destinations.

- true—Users can add, edit, and delete remote destinations.
- false (default)—Users cannot add, edit, and delete remote destinations.

Example: `<UserDefinedRemoteDestinations>>true</UserDefinedRemoteDestinations>`

Voicemail_Enabled

Applies to all the Cisco Jabber clients.

Enables voicemail capabilities and user interface in the client.

- true (default)—Enables voicemail capabilities and user interface.
- false—Disables voicemail capabilities and user interface.

Example: `<Voicemail_Enabled>>false</Voicemail_Enabled>`

VoiceServicesDomain

Applies to all the Cisco Jabber clients.

Specifies the Fully Qualified Domain Name that represents the DNS domain where the DNS SRV records for `_collab-edge` and `_cisco-uds` are configured.

Example: Given the following DNS SRV records:

- `_collab-edge._tls.voice.example.com`
- `_cisco-uds._tcp.voice.example.com`

The VoiceServicesDomain value will be `voice.example.com`.

WhitelistBot

Applies to all the Cisco Jabber clients.

Only Bots listed in WhitelistBot are allowed to start group chats, conference calls or join instant meetings. If WhitelistBot configuration parameter is not defined, the default will be the JIDs defined in AdminConfiguredBot.

Cisco Jabber allows regular expressions in WhitelistBot, like the * special character. For example * would open "robot-type" messages coming from any client, or {bot}*{@cisco.com} would whitelist JIDs beginning with bot, for example, bot1@cisco.com, bot_thisworks@cisco.com.

Example:<WhitelistBot>bot1@example.com;bot2@example.com;bot3@example.com</WhitelistBot>



CHAPTER 8

Presence

- [DomainsForOutlookPresence](#), on page 81
- [CalendarWebExMeetingPresence](#), on page 81
- [EnableOutlookPresenceIntegration](#), on page 82
- [meetingservice_supportmultimeeting](#), on page 82
- [LoginResource](#), on page 82
- [OutlookContactResolveMode](#), on page 82
- [PresenceServerAddress](#), on page 83
- [PresenceServerURL](#), on page 83

DomainsForOutlookPresence

Applies to Cisco Jabber for desktop clients.

Specifies that if you configure a domain with this key, you'll be able to see presence information for people only within the specified domain. If not configured, you'll be able to see presence information for all the contacts (domains).

This key supports multiple whitelisted domains which are separated by comma. For example `<DomainsForOutlookPresence>cisco.com, cisco.cn</DomainsForOutlookPresence>`.

It supports simple wildcard match. For example, `*.cisco.com` or `*cisco.com`.

Example: `<DomainsForOutlookPresence>cisco.com</DomainsForOutlookPresence>`

CalendarWebExMeetingPresence

Applies to Cisco Jabber for Windows.

Enables users' presence to change to "In a Webex meeting" even if they do not join the Cisco Webex session link but the meeting is in their Microsoft Outlook calendar.

- `true` - Users' presence changes to "In a Webex meeting" even if they do not join the Cisco Webex session link.
- `false` (default) - Users must join the Cisco Webex session link for their presence to change to "In a Webex meeting". Otherwise, their presence remains "Available", even if the meeting is in their Microsoft Outlook calendar.

Example: `<CalendarWebExMeetingPresence>>true</CalendarWebExMeetingPresence>`

EnableOutlookPresenceIntegration

Applies to Cisco Jabber for Mac

Prerequisite: Microsoft Outlook 15.34.0

Specifies if presence in Cisco Jabber is integrated with Microsoft Outlook.

- True (default)—Users' presence in Cisco Jabber is integrated with Microsoft Outlook.
- False—Users' presence in Cisco Jabber is not integrated with Microsoft Outlook.

meetingservice_supportmultimeeting

Applies to Cisco Jabber for Windows.

Specifies if Jabber is allowed to start multiple Webex Meetings.

- true (default)—Enable multiple meetings
- false—Disable multiple meetings

Example: `<meetingservice_supportmultimeeting>>true</meetingservice_supportmultimeeting>`

LoginResource

Applies to all the Cisco Jabber clients.

This parameter controls whether users can sign in to multiple Cisco Jabber client instances.

- multiResource (default)—Users can sign in to multiple instances of the client at the same time.
- wbxconnect—Users can sign in to one instance of the client at a time. This option applies to cloud and hybrid deployments only.

The client appends the `wbxconnect` suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the `wbxconnect` suffix.

- mutualExclusion—Users can sign in to one instance of the client at a time. This option applies to all deployment types (on-premises, cloud, and hybrid). New sign ins automatically sign out users from older instances of the client.

Example: `<LoginResource>mutualExclusion</LoginResource>`

OutlookContactResolveMode

Applies to Cisco Jabber for Windows and Mac

Specifies how Jabber resolves the presence of a contact in Outlook.

- **Auto** (default)—When you configure the `proxyaddress` attribute with `SIP:user@cupdomain`, then Jabber uses `user@cupdomain` as a Jabber ID. If you configure the `proxyaddress` attribute without SIP, Jabber uses an email address to resolve the presence of a contact in Outlook.
- **Email**—When you configure the `proxyaddress` attribute with `SIP:user@cupdomain`, then Jabber uses `user@cupdomain` as an email address. If you configure the `proxyaddress` attribute without SIP, Jabber uses an email address to resolve the presence of a contact in Outlook.

Example: `<OutlookContactResolveMode>Email</OutlookContactResolveMode>`

PresenceServerAddress

Applies to all the Cisco Jabber clients.

Specifies the address of a presence server for on-premises deployments. Set one of the following as the value:

- Hostname (*hostname*)
- IP address (*123.45.254.1*)
- FQDN (*hostname.domain.com*)

Example: `<PresenceServerAddress>hostname</PresenceServerAddress>`

PresenceServerURL

Applies to all the Cisco Jabber clients.

Specifies the Central Authentication Service (CAS) URL for the Cisco Webex Messenger service.

Example:

`<PresenceServerURL>https://login.webexconnect.com/cas/sso/ex_org/orgadmin.app</PresenceServerURL>`



CHAPTER 9

Voicemail

- [ForwardVoicemail](#), on page 85
- [VoicemailBackup1Server](#), on page 85
- [VoicemailBackup2Server](#), on page 86
- [VoicemailPrimaryServer](#), on page 86
- [VoiceMailService_UseCredentialsFrom](#), on page 86

ForwardVoicemail

Applies to all clients.

Determines whether users can forward voicemails from the **Voice Messages** tab.

- true (default)—voicemail forwarding is enabled. When users select a voicemail in the **Voice Messages** tab, the **Forward voice message** option is available.
- false—voicemail forwarding is not enabled.

Example: `<ForwardVoicemail>>false</ForwardVoicemail>`

VoicemailBackup1Server

Applies to Cisco Jabber for desktop and mobile clients.

Specifies the first backup server that the client connects to if the primary server is down or unreachable. You can specify the following values:

- Hostname (*hostname*)
- IP Address (*123.45.254.1*)
- FQDN (*hostname.domain.com*)

The Cisco Jabber client supports having two backup servers, plus the primary server, totaling three servers. However, the voicemail server supports only two voicemail servers in one cluster. To configure two backup servers, put one in the same cluster as the primary server, and the second in another cluster

Example: `<VoicemailBackup1Server>hostname</VoicemailBackup1Server>`

VoicemailBackup2Server

Applies to Cisco Jabber for desktop and mobile clients.

Specifies the second backup server that the client connects to if the primary server is down or unreachable. You can specify the following values:

- Hostname (*hostname*)
- IP Address (*123.45.254.1*)
- FQDN (*hostname.domain.com*)

The Cisco Jabber client supports having two backup servers plus the primary server, totaling three servers. However, the voicemail server supports only two voicemail servers in one cluster. To configure two backup servers, put one in the same cluster as the primary server, and the second in another cluster.

Example: `<VoicemailBackup2Server>hostname.domain.com</VoicemailBackup2Server>`

VoicemailPrimaryServer

Applies to all the Cisco Jabber clients.

Specifies the address of your voicemail server. Set one of the following as the value:

- Hostname (*hostname*)
- IP address (*123.45.254.1*)
- FQDN (*hostname.domain.com*)

Example: `<VoicemailPrimaryServer>hostname</VoicemailPrimaryServer>`

VoiceMailService_UseCredentialsFrom

Applies to all the Cisco Jabber clients.

Specifies that the client uses the phone service credentials to access voicemail services.

Ensure the user's phone service credentials match their voicemail service credentials. If you set this configuration, users cannot specify voicemail service credentials in the client interface.

This parameter is not set by default. The value is phone.

You should set this parameter in the following deployments only:

- Hybrid cloud-based deployments.
- Phone mode deployments.

In on-premises deployments, set the credentials source on the presence server for voicemail services.

The following is an example of the voicemail service credentials parameter:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Voicemail>
    <VoiceMailService_UseCredentialsFrom>phone</VoiceMailService_UseCredentialsFrom>
  </Voicemail>
</config>
```




CHAPTER 10

Directory Integration

- [Directory Parameters, on page 89](#)
- [CDI Parameters, on page 91](#)
- [Attribute Mapping Parameters, on page 102](#)
- [UDS Parameters, on page 104](#)
- [Directory Server Configuration Examples, on page 106](#)

Directory Parameters

The following table lists the BDI and EDI parameters, indicating the CDI parameter name or if it doesn't apply to Jabber 11.8 or later.

BDI Parameters	EDI Parameters	CDI Parameters
-	DirectoryServerType	DirectoryServerType
-	ConnectionType	-
BDILDAPServerType	-	-
BDIPresenceDomain	PresenceDomain	PresenceDomain
BDIPrimaryServerName	PrimaryServerName	PrimaryServerName
-	SecondaryServerName	SecondaryServerName
BDIServerPort1	ServerPort1	ServerPort1
-	ServerPort2	ServerPort2
-	UseWindowCredentials	-
BDIUseJabberCredentials	-	-
BDIConnectionUsername	ConnectionUsername	ConnectionUsername
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL

BDI Parameters	EDI Parameters	CDI Parameters
-	UseSecureConnection	-
BDIUseANR	UseANR	UseANR
BDIBaseFilter	BaseFilter	BaseFilter
BDIGroupBaseFilter	GroupBaseFilter	GroupBaseFilter
BDIUseANR	-	-
BDIPredictiveSearchFilter	PredictiveSearchFilter	PredictiveSearchFilter
-	DisableSecondaryNumberLookups	DisableSecondaryNumberLookups
-	SearchTimeout	SearchTimeout
-	UseWildcards	UseWildcards
-	MinimumCharacterQuery	MinimumCharacterQuery
BDISearchBase1	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5
BDIGroupSearchBase1	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5
BDIUseSipUriToResolveContacts	UseSipUriToResolveContacts	UseSipUriToResolveContacts
BDIUriPrefix	UriPrefix	UriPrefix
BDISipUri	SipUri	SipUri
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	PhotoUriSubstitutionToken
BDIPhotoUriWithToken	PhotoUriWithToken	PhotoUriWithToken
BDIPhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName

BDI Parameters	EDI Parameters	CDI Parameters
BDIFirstname	Firstname	Firstname
BDILastname	Lastname	Lastname
BDIEmailAddress	EmailAddress	EmailAddress
BDISipUri	SipUri	SipUri
BDIPhotoSource	PhotoSource	PhotoSource
BDIBusinessPhone	BusinessPhone	BusinessPhone
BDIMobilePhone	MobilePhone	MobilePhone
BDIHomePhone	HomePhone	HomePhone
BDIOtherPhone	OtherPhone	OtherPhone
BDIDirectoryUri	DirectoryUri	DirectoryUri
BDITitle	Title	Title
BDICompanyName	CompanyName	CompanyName
BDIUserAccountName	UserAccountName	UserAccountName
BDIDomainName	DomainName	DomainName
BDICountry	Country	Country
BDILocation	Location	Location
BDINickname	Nickname	Nickname
BDIPostalCode	PostalCode	PostalCode
BDICity	City	City
BDIState	State	State
BDIStreetAddress	StreetAddress	StreetAddress

CDI Parameters

The CDI parameters apply to all clients.

Directory Connection

PrimaryServerName

Specifies the address of the primary directory server. You can configure this parameter to enable manual connection where the client cannot automatically discover the directory server.



Note The client attempts to connect to the primary directory server or the secondary directory server in the following ways:

- When the client starts, it attempts to connect to the primary server.
- The client attempts to connect to the secondary server when:
 - The primary server is not available.
 - The primary server fails after the client connects to it.
- If the connection to the secondary server is successful, the client retains the connection to the secondary server until the next restart.
- If the secondary server fails while the client is connected to it, the client attempts to connect to the primary server.

-
- IP address — Use IP address for primary directory server.
 - FQDN — Use FQDN for primary directory server.

Example: `<PrimaryServerName>parent-domain-fqdn</PrimaryServerName>`

SecondaryServerName

Specifies the address of the backup directory server.

You must configure this parameter to enable manual connections where the client cannot automatically discover the directory server.

When you specify a value for the PrimaryServerName parameter, you must configure this parameter for failover.

- IP address—Use IP address for backup directory server.
- FQDN—Use FDQN for backup directory server.

Example: `<SecondaryServerName>www.example.com</SecondaryServerName>`

ServerPort1

Specifies the port for the primary directory server.

When you specify a value for the PrimaryServerName parameter, you must configure this parameter.

Example: `<ServerPort1>123</ServerPort1>`

ServerPort2

Specifies the port for the backup directory server.

When you specify a value for the SecondaryServerName parameter, you must configure this parameter.

Example: <ServerPort2>345</ServerPort2>

ConnectionUsername

Lets you manually specify a shared username that the client can use to authenticate with the directory server.

By default, Jabber desktop clients use Kerberos or client certificate authentication. Only use this parameter in deployments where you can't authenticate with the directory server using either Kerberos or client certificate authentication.

You must use only a well-known or public set of credentials for an account with read-only permissions to the directory.



Important

The client transmits and stores this username as plain text.

Example: <ConnectionUsername>username</ConnectionUsername>

ConnectionPassword

Lets you manually specify a shared password that the client can use to authenticate with the directory server.

By default, Jabber desktop clients use Kerberos or client certificate authentication. Only use this parameter in deployments where you can't authenticate with the directory server using either Kerberos or client certificate authentication.

You must use only a well-known or public set of credentials for an account with read-only permissions to the directory.



Important

The client transmits and stores this password as encrypted unless you have configured your LDAP settings for plaintext transmission.

The value for this parameter is the shared password.

Example: <ConnectionPassword>password</ConnectionPassword>

UseSSL

Default setting: True

The connection to the LDAP server uses SSL by default using the LDAPS protocol.

Setting this to False uses the plaintext LDAP protocol. The plaintext LDAP protocol will also be chosen if the LDAP port is either 389 or 3268 and the UseSSL configuration key is not set.



Note The configuration key when set overrides any automatic determination of the protocol.

UseANR

Default setting (all clients): True

Enable/disable the use of Ambiguous Name Resolution (ANR) when performing predictive search queries.

When set to True, Jabber constructs LDAP queries using ANR for predictive search.

If set to False, Jabber constructs a complex query for use in predictive search.

ANR is disabled if Jabber is connecting to an OpenLDAP server. It is enabled only when connecting to an Active Directory server.

The format of the query used for non-ANR servers is set using the “PredictiveSearchFilter” parameter.

Example: `<UseANR>>false</UseANR>`

Directory Query

BaseFilter

Specifies a base filter for Active Directory queries.

You must specify a directory subkey name if you want to retrieve objects other than user objects when you query the directory.

Configuration files can contain only valid XML character entity references. To specify a custom base filter, you must use `&` instead of `&`.

The default value for all clients is `(&(objectCategory=person) (objectClass=user))`.

Example: `<BaseFilter>(&(objectCategory=person) (memberOf=cn=group-name))</BaseFilter>`

GroupBaseFilter

Specifies a base filter for Active Directory Enterprise Group queries.

The default value for all clients is:

`(&(objectCategory=group) (! (groupType:1.2.840.113556.1.4.803:=2147483648))`
(ensure you remove any spaces inserted in this value prior to using it).

Example:

`<GroupBaseFilter>(&(objectCategory=person) (memberOf=cn=group-name))</GroupBaseFilter>`

PredictiveSearchFilter

Defines the attribute set for predictive search LDAP queries. You can define multiple, comma-separated values to filter search queries.

This setting is only read when “UseANR” is set to False, or when connecting to a non-Active Directory server. If UseANR is not set to any value, Jabber will use a default attribute set for predictive search queries.

Default values are created based on attribute mappings for the following Jabber parameters:

- mail
- username
- displayname
- givenname
- surname
- nickname
- sipURI

Typical mappings for these attributes are as follows:

Jabber Parameter	Active Directory attribute	OpenLDAP
mail	mail	mail
username	SAMAccountName	uid
displayname	displayName	cn
givenname	givenName	givenName
nickname	displayName	
sipURI	msRTCSIP-PrimaryUserAddress	mail
surname	sn	sn

If your directory server doesn't support ANR format queries, you can populate this setting if you want to customize the attribute set queried for predictive search queries.

DisableSecondaryNumberLookups

Specifies whether users can search for alternative contact numbers if the work number is not available, such as the mobile, home, or other number.

- 0 (default) — Users can search for alternative contact numbers.
- 1 — Users cannot search for alternative contact numbers.

Example: `<DisableSecondaryNumberLookups>1</DisableSecondaryNumberLookups>`

SearchTimeout

Specifies the timeout period for queries in seconds.

The value for this parameter is number of seconds. The default value is 5.

Example: `<SearchTimeout>6</SearchTimeout>`

MinimumCharacterQuery

Sets the minimum number of characters in a contact name that a user needs to enter to query the name from the directory.

The only value for this parameter is a numerical value. The default value is 3.

For example, if you set 2 as the value of this parameter, the client searches the directory when users enter at least two characters in the search field.

Example: `<MinimumCharacterQuery>2</MinimumCharacterQuery>`

SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5

Specifies a location in the directory server from which searches begin.

A search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree.

Active Directory doesn't typically require a search base. Specify search bases for Active Directory only when you have specific performance requirements. When specifying search bases, you must also specify search base for directory servers other than Active Directory to create bindings to specific locations in the directory.

The value for this parameter is a searchable Organizational Unit (OU) in the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior.



Tip You can specify an OU to restrict searches to certain user groups. For example, a subset of your users has IM capabilities only. Include those users in an OU and then specify that as a search base.

Example: `<SearchBase1>OU=Users1</SearchBase1>`

GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5

Specifies a location in the directory server from which Enterprise Group searches begin.

A search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree.

You can specify the value of up to five search bases in your Organizational Unit (OU) to override the default behavior.

The value for this parameter is a searchable OU in the directory tree.

Example: `<GroupSearchBase1>OU=Group1</GroupSearchBase1>`

IM Address Scheme

UseSipUriToResolveContacts

Specifies the IM address scheme that the Cisco IM and Presence service uses.

- true — Use the Directory URI scheme.
- false (default) — Use the User ID @[Default Domain] scheme.

Example: `<UseSipUriToResolveContacts>true</UseSipUriToResolveContacts>`

UriPrefix

Specifies a prefix to remove from the SipUri parameter.

The value is a prefix string.

For example, sip: may prefix the msRTCSIP-PrimaryUserAddress directory attribute.

Example: `<UriPrefix>sip:</UriPrefix>`

SipUri

Specifies the directory attribute field that the IM Address scheme field is mapped to.

The value for this parameter can be one of the following directory attribute fields:

- mail
- msRTCSIP-PrimaryUserAddress

Example: `<SipUri>msRTCSIP-PrimaryUserAddress</SipUri>`

LdapSupportedMechanisms

Applies to all clients.

Specifies the order for authenticating with the LDAP server.

Each of the mechanisms specified below must be supported by the Contact Service and the LDAP server.

Use a space to separate multiple authentication mechanisms.

- **GSSAPI (default)**—Kerberos v5. Supported by desktop clients only.
- **EXTERNAL**—SASL external.
- **PLAIN**—Simple LDAP bind (anonymous bind is a subset of simple bind). Used by default if ConnectionUsername and ConnectionPassword parameters or LDAP_UseCredentialsFrom parameter are present

Example 1: `<LdapSupportedMechanisms>GSSAPI EXTERNAL PLAIN</LdapSupportedMechanisms>`

In this example, Jabber checks first if GSSAPI is supported, then attempts to authenticate. If GSSAPI is not supported, then Jabber checks if EXTERNAL is supported, then attempts to authenticate. If neither are supported, then Jabber attempts PLAIN authentication.

Example 2: `<LdapSupportedMechanisms>PLAIN</LdapSupportedMechanisms>`

In this example, Jabber uses PLAIN authentication only.

EnableEmployeeNumber

Applies to Cisco Jabber for Windows.

Fetches the employee number from the LDAP server when a user searches for it using Jabber.

- 0 or false (default)—Employee number is disabled.

- 1 or true—Employee number is enabled.

Example: `<EnableEmployeeNumber>0</EnableEmployeeNumber>`

UseLdapReferral

Applies to Cisco Jabber for Windows and Cisco Jabber for Android.

Specifies if the client uses LDAP referrals when attempting to resolve contacts.

Values:

- 0 (Default)—Disables LDAP referrals
- 1—Enables LDAP referrals

Example: `<UseLdapReferral>1</UseLdapReferral>`

LDAP_UseCredentialsFrom

Applies to all Cisco Jabber clients for on-premises deployments.

Specifies which credentials are used by Cisco Jabber when connecting to the directory server.

- Voicemail—use voicemail credentials when connecting to the directory server.
- Exchange—use the credentials that Cisco Jabber uses to connect to Microsoft Exchange when connecting to the directory server.
- CUCM—use Cisco Unified Communications Manager credentials when connecting to the directory server.

Example: `<LDAP_UseCredentialsFrom>CUCM</LDAP_UseCredentialsFrom>`

When this parameter is set, users are not given the option to enter their directory credentials manually in the Options window. You can also set directory credentials using the Cisco Unified Communications Manager service profile or using the CDI directory integration parameters you defined in the `jabber-config.xml` file. It is not recommended to use both synchronized credentials and administrator-defined credentials.

Keep in mind that you may need to use the `LdapUserDomain` parameter to define the domain to authenticate against the LDAP server (where applicable). For example, the authentication ID would be `<CUCM Username>@<LdapUserDomain>`.



Note Do not use the `LDAP_UseCredentialsFrom` parameter with any of the following parameters because they can cause conflicting configuration:

- `LdapAnonymousBinding`
 - `ConnectionUsername` and `ConnectionPassword`
 - `UseWindowsCredentials`
-

LdapUserDomain

Applies to all Cisco Jabber clients for on-premises deployments.

Specifies the domain to be appended to the username when connecting to the LDAP server. This is useful when the LDAP server requires a UPN or email-based account to authenticate with. This parameter is used with the LDAP_UseCredentialsFrom parameter.

The username is appended with the @ symbol followed by the value specified by LdapUserDomain. This value is then used to connect to the LDAP server. For example, a user named Adam McKenzie has the user ID *amckenzie* and the LdapUserDomain is *example.com*, then the username that authenticates with the LDAP server is *amckenzie@example.com*.

Example: `<LdapUserDomain>example.com</LdapUserDomain>`

Contact Photo

PhotoUriSubstitutionEnabled

Specifies if a URI is used to display photos.

- true — Photo URI substitution is enabled.
- false (default) — Photo URI substitution is disabled.

Example: `<PhotoUriSubstitutionEnabled>true</PhotoUriSubstitutionEnabled>`

PhotoUriSubstitutionToken

Specifies the token in the Photo URI that is used to create the path to the photos.

Only the following attributes are supported for use with the PhotoURISubstitutionToken parameter:

- Common Name
- Display Name
- First Name
- Last Name
- Nickname
- Email Address
- Photo Source
- Business Phone
- Mobile Phone
- Home Phone
- Preferred Phone
- Other Phone
- Title

- Company Name
- User Account Name
- Domain Name
- Location
- Post Code
- State
- City
- Street

**Important**

When using this parameter, you must ensure the PhotoUriSubstitutionEnabled parameter is set to true.

The value for this parameter is a directory attribute.

Example: `<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>`

PhotoUriWithToken

Specifies a photo URI with a directory attribute as a variable value.

The parameter applies to LDAP directory integrations.

**Restriction**

The client must be able to retrieve the photos from the web server without credentials.

To configure photo URI substitution, you set the directory attribute as the value of PhotoUriSubstitutionToken.

The value for this parameter is a URI.

Example:

`<PhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</PhotoUriWithToken>`

PhotoSource

The name of a directory attribute that stores a contact photo as a binary object or a URI to a contact photo.

The value is a directory attribute.

Example: `<PhotoSource>thumbnailPhoto</PhotoSource>`

**Tip**

If you are using attributes such as “jpegPhoto” and “thumbnailPhoto”, ensure that these are added to the Global Catalog on the Active Directory.

PhoneNumberMasks

Specifies masks to use when users search for phone numbers.

For example, a user receives a call from +14085550100. In the directory, this number is +(1) 408 555 0100. The following mask resolves the number: +1408|+(#) ### ### ####. The length of mask strings cannot exceed the size restriction for registry subkey names.

Phone masks apply to phone numbers before the client searches your directory. If you configure phone masks correctly, directory searches succeed as exact query matches and prevents any impact on the performance of your directory server.

The following table describes the elements you can include in a phone mask:

Element	Description
Phone number pattern	<p>Provides a number pattern to retrieve phone numbers from your directory.</p> <p>To add a phone mask, you specify a number pattern that applies to the mask. For example, to specify a mask for searches that begin with +1408, you can use the following mask: +1408 +(#) ### ### ####.</p> <p>To enable a mask to process phone numbers that have the same number of digits, but different patterns, use multiple masks with the same number of digits. For example, your company has site A and site B. Each site maintains a separate directory in which the phone numbers have different formats, such as the following:</p> <p style="padding-left: 40px;">+(1) 408 555 0100 +1-510-5550101</p> <p>The following mask ensures you can use both numbers correctly: +1408 +(#) ### ### #### +1510 +##-#####.</p>
Pipe symbol ()	<p>Separates number patterns and masks.</p> <p>For example, +1408 +(#) ### ### #### +34 +(##) ### ####.</p>
Wildcard character	<p>Substitutes one or more characters with a subset of possible matching characters.</p> <p>Any wildcard character can exist in a phone mask. For example, an asterisk (*) represents one or more characters and can apply to a mask as follows: +3498 +##*###*#####.</p> <p>Using this mask with the wildcard, a phone number search can match any of the following formats:</p> <p style="padding-left: 40px;">+34(98)555 0199 +34 98 555-0199 +34-(98)-555.0199</p>
Reverse mask	<p>Applies a number pattern from right to left.</p> <p>For example, a mask of +3498 R+34 (98) 559 ##### applied to +34985590199 results in +34 (98) 559 0199.</p> <p>You can use both forward and reverse masks.</p>

The only value for this parameter is mask string.

Example: <PhoneNumberMasks>+1408|+(#) ### ### ####</PhoneNumberMasks>

Attribute Mapping Parameters

The following table describes the parameters for mapping LDAP directory attributes.

CDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
CommonName	cn	Yes	Yes	No
DisplayName	displayName	Yes	Yes	Yes
Firstname	givenName	Yes	Yes	Yes
Lastname	sn	Yes	Yes	Yes
EmailAddress	mail	Yes	Yes	Yes
SipUri Note The client uses this parameter for intradomain federation, not URI dialing.	msRtCSIP-PrimaryUserAddress	Yes	Yes	Yes
PhotoSource	thumbnailPhoto	No	No	No
BusinessPhone	telephoneNumber	Yes	No	No
MobilePhone	mobile	Yes	No	No
HomePhone	homePhone	Yes	No	No
OtherPhone	otherTelephone	Yes	No	No
DirectoryUri Note The client uses this parameter for URI dialing.	mail	Yes	No	No
Title	title	Yes	No	No
CompanyName	company	Yes	Yes	No
UserAccountName	sAMAccountName	Yes	Yes	Yes
DomainName	userPrincipalName	Yes	Yes	No
	co	Yes	No	No
Location		Yes	No	No

CDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
Nickname	displayName	Yes	Yes	Yes
PostalCode	postalCode	Yes	No	No
City	l	Yes	Yes	No
State	st	Yes	Yes	No
StreetAddress	streetAddress	Yes	No	No

Attributes on the Directory Server

You must index attributes on your LDAP directory server for the clients. This lets clients resolve contacts.

To use the default attribute mappings, you must index the following attributes:

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

Additionally, you must index the following attributes for secondary number queries:

- otherTelephone
- mobile
- homePhone



Note By default secondary number queries are enabled in Cisco Jabber for Windows. You can disable secondary number queries with the DisableSecondaryNumberLookups parameter.

- msRTCSIP-PrimaryUserAddress

Since Cisco Jabber for Windows connects to a Global Catalog server by default, you must ensure that all attributes reside on your Global Catalog server. You can replicate attributes to a Global Catalog server using an appropriate tool such as the Microsoft Active Directory Schema Snap-in. You can choose either to replicate or not to replicate attributes to your Global Catalog server:

- If you replicate attributes to your Global Catalog server, it generates traffic between Active Directory servers in the domain. For this reason, you should replicate attributes to your Global Catalog server only if the network traffic can handle extra load.
- If you do not want to replicate attributes to a Global Catalog server, configure Cisco Jabber to connect to a Domain Controller. In this case, the client queries single domains only when it connects to a Domain Controller.

UDS Parameters

Use the UDS parameters to connect to the UDS server and to perform contact resolution and directory queries.

The UDS parameters apply to all the Cisco Jabber clients.

Directory Connection

PresenceDomain

Specifies the domain of the presence node. This is a required parameter.

The only value for this parameter is domain of the presence node.

The client adds this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the user ID *amckenzie*. You specify *example.com* as the presence node domain.

When the user logs in, the client constructs the IM address *amckenzie@example.com* for Adam McKenzie.

Example: `<PresenceDomain>example.com</PresenceDomain>`

UdsServer

Specifies the address of the Cisco Unified Communications Manager User Data Service (UDS) server.

This parameter is required for manual connections where the client cannot automatically discover the UDS server.

- IP address — Use IP address for UDS server.
- FQDN — Use FQDN for UDS server.

Example: `<UdsServer>ccm1</UdsServer>`

IM Address Scheme

UdsPhotoUriWithToken

Specifies a photo URI with a directory attribute as a variable value.

This parameter applies to UDS directory integrations. You must specify this parameter to download contact photos in either of the following cases:

- If you configure the `DirectoryServerType` parameter to use UDS. With this configuration, the client uses UDS for contact resolution when it is inside or outside the corporate firewall.
- If you deploy Expressway for Mobile and Remote Access. With this deployment, the client automatically uses UDS for contact resolution when it is outside the corporate firewall.



Restriction

The client must be able to retrieve the photos from the web server without credentials.

The value for this parameter is a URI.

Example: `<UdsPhotoUriWithToken>http://www.photo/url/path/%%uid%.jpg</UdsPhotoUriWithToken>`

UseSIPURIToResolveContacts

Specifies the IM address scheme that the IM and Presence Service uses.

- `true` — Use the Directory URI scheme.
- `false` (default) — Use the User ID `@[Default Domain]` scheme.

Example: `<UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>`

UriPrefix

Specifies a prefix to remove from the `SipUri` parameter.

The only value is a prefix string.

For example, `sip:` may prefix the `msRTCSIP-PrimaryUserAddress` directory attribute.

If `SipUri` is not set to `msRTCSIP-PrimaryUserAddress`, delete the tag `<UriPrefix>sip:</UriPrefix>`

Example: `<UriPrefix>sip:</UriPrefix>`

SipUri

Specifies the directory attribute field to which the IM Address scheme field is mapped.

The value for this parameter can be one of the following directory attribute fields:

- `mail`
- `msRTCSIP-PrimaryUserAddress`

Example: `<SipUri>msRTCSIP-PrimaryUserAddress</SipUri>`

EmailAddress

Applies to all the Cisco Jabber clients.

Specifies which attribute in User Data Service (UDS) is the email address. Configure this parameter with the value mail.

Example:

```
<EmailAddress>mail</EmailAddress>
```



Note This parameter supports both LDAP and UDS queries in the latest Jabber versions.

MaxWordsOfFirstName

Applies to all the Cisco Jabber clients.

This parameter applies to UDS directory integrations and specifies the maximum number of words that a user's first name can have in the predictive search. The default value for a user's first name is 2 words and there is no limit for the maximum words.

Example: `<MaxWordsOfFirstName>2</MaxWordsOfFirstName>`

MaxWordsOfLastName

Applies to all the Cisco Jabber clients.

This parameter applies to UDS directory integrations and specifies the maximum number of words that a user's last name can have in the predictive search. The default value for a user's last name is 2 words and there is no limit for the maximum words.

Example: `<MaxWordsOfLastName>2</MaxWordsOfLastName>`

Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

Domain Controller Connection

To connect to a Domain Controller, set the following parameters:

Parameter	Value
ConnectionType	1

The following is an example configuration:

```
<Directory>
<ConnectionType>1</ConnectionType></Directory>
```

KerberosConfiguration

Applies to Cisco Jabber for desktop

You can add the KerberosConfiguration parameter in the jabber-config.xml file. The parameter value is written to the disk as the MIT-Kerberos configuration file.

If you don't configure this parameter, Jabber can only connect to the Active Directory domain joined by the client machine to perform a directory search. To connect to other Active Directory domains to which the client machine doesn't belong, configure domain_realm mapping.

For example, in a Multi-Forest environment, suppose you have two forests deployed in your AD infrastructure. The user accounts are in forest 1 and the resource is in forest 2. In this case, configure domain1.com as the user domain and configure domain2.com and child.domain2.com as the resource domain. You establish a trust relationship between forest 1 and forest 2.

If users sign in from domain1.com and want to access the resource domain, configure KerberosConfiguration with the appropriate values in jabber-config.xml.



Note If the Kerberos configuration doesn't work when typed in a single line, try typing it in multiple lines as in this example.

Example:

```
<Directory>
  <KerberosConfiguration>
    [domain_realm]
    .domain1.com = DOMAIN1.COM
    .child.domain1.com = CHILD.DOMAIN1.COM
  </KerberosConfiguration>
</Directory>
```

Manual Server Connections for Cisco Jabber

To manually connect to a directory server, set the following parameters:

Parameter	Value
PrimaryServerName	FQDN IP address
ServerPort1	Port number
SecondaryServerName	FQDN IP address
ServerPort2	Port number

The following is an example configuration:

```
<Directory>
<PrimaryServerName>primary-server-name.domain.com</PrimaryServerName>
<ServerPort1>1234</ServerPort1>
<SecondaryServerName>secondary-server-name.domain.com</SecondaryServerName>
<ServerPort2>5678</ServerPort2>
</Directory>
```

UDS Integration

To integrate with UDS, set the following parameters.

Parameter	Value
DirectoryServerType	UDS
UdsServer	IP address of the UDS server
UdsPhotoUriWithToken	Contact photo URL
PresenceDomain	Server address of your presence domain
Note	This parameter is only applicable to Phone Mode.



Note Configure the DirectoryServerType parameter to UDS only if you want to use UDS for all contact resolution (that is, from inside and outside the corporate firewall).

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>UDS</DirectoryServerType>
  <UdsServer>11.22.33.444</UdsServer>
  <UdsPhotoUriWithToken>http://server-name/%%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```

LDAP Integration with Expressway for Mobile and Remote Access

When you deploy Expressway for Mobile and Remote Access with an LDAP directory integration, the client uses:

- LDAP when inside the corporate firewall
- UDS when outside the corporate firewall



Note LDAP is the default configuration, so it is not necessary to include the DirectoryServerType parameter in your client configuration file.

To ensure that the client can resolve contact photos from both inside and outside your corporate firewall, set the following parameters.

Parameter	Value
PhotoUriWithToken	Contact photo URL when inside the corporate firewall.
UdsPhotoUriWithToken	contact photo URL when outside the corporate firewall.

The following is an example configuration:

```
<Directory>
  <PhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</PhotoUriWithToken>
  <UdsPhotoUriWithToken>http://server-name/%%uid%.jpg</UdsPhotoUriWithToken>
</Directory>
```

Simple Authentication for Cisco Jabber

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword> password</ConnectionPassword>
```

