Phone

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 all 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 it 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 it 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 authentication by fingerprint or facial recognition 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 or facial recognition. 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 authentication by fingerprint or facial recognitionfingerprint or facial recognition. The users can decide if they want to use biometric authentication to sign into Cisco Jabber.
- AdminDisabled—Cisco Jabber doesn't use authentication by fingerprint or facial recognition. 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>`

UseSIPforMobiles

Applies to Cisco Jabber for mobile clients.

Specifies that SIP URIs are always shown, even if in the same domain.

- true—Always show SIP URI, even for the same domain.
- false (default)—Show domain name for the same domain, and show SIP URI for different domains.