Configure Cisco Jabber

Learn how to configure Cisco Jabber and review the configuration parameters you can set.

- Introduction to Client Configuration, page 1
- Configure Client on Cisco Unified Communications Manager, page 2
- Create and Host Client Configuration Files, page 7
- Configuration File Structure, page 14
- Summary of Configuration Parameters, page 16
- Client Parameters, page 17
- Options Parameters, page 18
- Phone Parameters, page 20
- Policies Parameters, page 23
- Presence Parameters, page 29
- Service Credentials Parameters, page 30
- Voicemail Parameters, page 30

Introduction to Client Configuration

Cisco Jabber can retrieve configuration settings from the following sources:

Service Profiles

You can configure some client settings in UC service profiles on Cisco Unified Communications Manager version 9 and higher. When users launch the client, it discovers the Cisco Unified Communications Manager home cluster using a DNS SRV record and automatically retrieves the configuration from the UC service profile.

Applies to on-premises deployments only.

Phone Configuration

You can set some client settings in the phone configuration on Cisco Unified Communications Manager version 9 and higher. The client retrieves the settings from the phone configuration in addition to the configuration in the UC service profile.

Applies to on-premises deployments only.

Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service

You can enable instant messaging and presence capabilities and configure certain settings such as presence subscription requests.

If you do not use service discovery with Cisco Unified Communications Manager version 9 and higher, the client retrieves UC services from Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service.

Applies to on-premises deployments only.

Client Configuration Files

You can create XML files that contain configuration parameters. You then host the XML files on a TFTP server. When users sign in, the client retrieves the XML file from the TFTP server and applies the configuration.

Applies to on-premises and cloud-based deployments.

Cisco WebEx Administration Tool

You can configure some client settings with the Cisco WebEx Administration Tool.

Applies to cloud-based deployments only.

Configure Client on Cisco Unified Communications Manager

You can configure some client settings in UC service profiles on Cisco Unified Communications Manager version 9 and higher.

Important

- Cisco Jabber only retrieves configuration from service profiles on Cisco Unified Communications Manager if the client gets the `_cisco-uds` SRV record from a DNS query.

  In a hybrid environment, if the CAS URL lookup is successful Cisco Jabber retrieves the configurations from Cisco WebEx Messenger service and the `_cisco-uds` SRV record is ignored.

- In an environment with multiple Cisco Unified Communications Manager clusters, you can configure the Intercluster Lookup Service (ILS). ILS enables the client to find the user's home cluster and discover services.

  If you do not configure ILS, then you must manually configure remote cluster information, similar to the EMCC remote cluster set up. For more information on Remote Cluster Configuration, see the Cisco Unified Communications Manager Features and Services Guide.

Set Parameters on Service Profile

The client can retrieve UC service configuration and other settings from service profiles.

Parameters in Service Profiles

Learn which configuration parameters you can set in service profiles. Review the corresponding parameters in the client configuration file.

IM and Presence Profile

The following table lists the configuration parameters you can set in the instant messaging and presence profile:

IM and Presence Service Configuration	Description
Product type	Provides the source of authentication to Cisco Jabber and has the following values: **Unified CM (IM and Presence)** Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service is the authenticator. **WebEx (IM and Presence)** The Cisco WebEx Messenger service is the authenticator. **Note** As of this release, the client issues an HTTP query in addition to the query for SRV records. The HTTP query allows the client to determine if it should authenticate to the Cisco WebEx Messenger service. As a result of the HTTP query, the client connects to the Cisco WebEx Messenger service in cloud-based deployments before getting the `_cisco-uds` SRV record. Setting the value of the **Product type** field to **WebEx** may have no practical effect if the WebEx service has already been discovered by a CAS lookup. **Not set** If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

IM and Presence Service Configuration	Description
Primary server	Specifies the address of your primary presence server. **On-Premises Deployments** You should specify the fully qualified domain name (FQDN) of Cisco Unified Presence or Cisco Unified Communications Manager IM and Presence Service. **Cloud-Based Deployments** The client uses the following URL as default when you select **WebEx** as the value for the **Product type** parameter: `https://loginp.webexconnect.com/cas/auth.do` This default URL overrides any value that you set.

Voicemail Profile

The following table lists the configuration parameters you can set in the voicemail profile:

Voicemail Service Configuration	Description
Voicemail server	Specifies connection settings for the voicemail server.
Credentials source for voicemail service	Specifies that the client uses the credentials for the instant messaging and presence or conferencing service to authenticate with the voicemail service. Ensure that the credentials source that you set match the user's voicemail credentials. If you set a value for this parameter, users cannot specify their voicemail service credentials in the client user interface.

Conferencing Profile

The following table lists the configuration parameters you can set in the conferencing profile:

Conferencing Service Configuration	Description
Conferencing server	Specifies connection settings for the conferencing server.
Credentials source for web conference service	Specifies that the client uses the credentials for the instant messaging and presence or voicemail service to authenticate with the conferencing service. Ensure that the credentials source that you set match the user's conferencing credentials.

Directory Profile

See the *Client Configuration for Directory Integration* chapter for information about configuring directory integration in a service profile.

CTI Profile

The following table lists the configuration parameters you can set in the CTI profile:

CTI Service Configuration	Description
CTI server	Specifies connection settings for the CTI server.

Add UC Services

Add UC services to specify the address, ports, protocols and other settings for services such as instant messaging and presence, voicemail, conferencing, and directory.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **UC Service**.
The **Find and List UC Services** window opens.

Step 3 Select **Add New**.
The **UC Service Configuration** window opens.

Step 4 Select the UC service type you want to add and then select **Next**.

Step 5 Configure the UC service as appropriate and then select **Save**.

What to Do Next

Add your UC services to service profiles.

Create Service Profiles

After you add and configure UC services, you add them to a service profile. You can apply additional configuration in the service profile.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **User Settings** > **Service Profile**.

The **Find and List UC Services** window opens.

Step 3 Select **Add New**.
The **Service Profile Configuration** window opens.

Step 4 Enter a name for the service profile in the **Name** field.

Step 5 Select **Make this the default service profile for the system** if you want the service profile to be the default for the cluster.

Note On Cisco Unified Communications Manager version 9.x only, users who have only instant messaging capabilities (IM only) must use the default service profile. For this reason, you should set the service profile as the default if you plan to apply the service profile to IM only users.

Step 6 Add your UC services, apply any additional configuration, and then select **Save**.

What to Do Next

Apply service profiles to end user configuration.

Apply Service Profiles

After you add UC services and create a service profile, you apply the service profile to users. When users sign in to Cisco Jabber, the client can then retrieve the service profile for that user from Cisco Unified Communications Manager.

Procedure

Step 1 Open the **Cisco Unified CM Administration** interface.

Step 2 Select **User Management** > **End User**.
The **Find and List Users** window opens.

Step 3 Enter the appropriate search criteria to find existing users and then select a user from the list.
The **End User Configuration** window opens.

Step 4 Locate the **Service Settings** section.

Step 5 Select a service profile to apply to the user from the **UC Service Profile** drop-down list.

Important **Cisco Unified Communications Manager version 9.x only:** If the user has only instant messaging and presence capabilities (IM only), you must select **Use Default**. For IM only users, Cisco Unified Communications Manager version 9.x always applies the default service profile regardless of what you select from the **UC Service Profile** drop-down list.

Step 6 Apply any other configuration as appropriate and then select **Save**.

Associate Users with Devices

On Cisco Unified Communications Manager version 9.x only, when the client attempts to retrieve the service profile for the user, it first gets the device configuration file from Cisco Unified Communications Manager. The client can then use the device configuration to get the service profile that you applied to the user.

For example, you provision Adam McKenzie with a CSF device named `CSFAKenzi`. The client retrieves `CSFAKenzi.cnf.xml` from Cisco Unified Communications Manager when Adam signs in. The client then looks for the following in `CSFAKenzi.cnf.xml`:

```
<userId  serviceProfileFile="identifier.cnf.xml">amckenzi</userId>
```

For this reason, if you are using Cisco Unified Communications Manager version 9.x, you should do the following to ensure that the client can successfully retrieve the service profiles that you apply to users:

- Associate users with devices.
- Set the **User Owner ID** field in the device configuration to the appropriate user. The client will retrieve the Default Service Profile if this value is not set.

Procedure

Step 1 Associate users with devices.

a) Open the **Unified CM Administration** interface.
b) Select **User Management** > **End User**.
c) Find and select the appropriate user.
The **End User Configuration** window opens.
d) Select **Device Association** in the **Device Information** section.
e) Associate the user with devices as appropriate.
f) Return to the **End User Configuration** window and then select **Save**.

Step 2 Set the **User Owner ID** field in the device configuration.

a) Select **Device** > **Phone**.
b) Find and select the appropriate device.
The **Phone Configuration** window opens.
c) Locate the **Device Information** section.
d) Select **User** as the value for the **Owner** field.
e) Select the appropriate user ID from the **Owner User ID** field.
f) Select **Save**.

Create and Host Client Configuration Files

In on-premises and hybrid cloud-based deployments you can create client configuration files and host them on the Cisco Unified Communications Manager TFTP service.

In cloud-based deployments, you should configure the client with the Cisco WebEx Administration Tool. However, you can optionally set up a TFTP server to configure the client with settings that are not available in Cisco WebEx Administration Tool.

Important In most environments, the client does not require any configuration to connect to services. You should create a configuration file only if you require custom content such as:

- Automatic updates
- Problem reporting
- User policies and options

Client Configuration Files

Before you deploy configuration files, review the differences between global and group configuration files. To successfully deploy configuration files you should also review the requirements for configuration files such as supported encoding.

Global Configuration Files

Global configuration files apply to all users. The client downloads the global configuration file from your TFTP server during the login sequence.

The default name for the global configuration file is `jabber-config.xml`.

Note Do not rename the jabber-config.xml file. The client does not support jabber-config.xml files with a different name.

Group Configuration Files

Note Group configuration files are supported on Cisco Jabber for Windows only.

Group configuration files apply to subsets of users. Group configuration files take priority over global configuration files.

Cisco Jabber retrieves group configuration files after users sign in to their phone account in the client for the first time. The client then prompts the users to sign out. During the second login sequence, the client downloads the group configuration file from your TFTP server.

Cisco Jabber loads group configuration files as follows:

Users are not signed in

1. Users sign in and then the client notifies the users about the change to their configuration settings.
2. Users sign out.
3. Users sign in and then the client loads the group configuration settings.

Users are signed in and use software phones for calls

1. The client notifies the users about the change to their configuration settings.
2. Users sign out.
3. Users sign in and then the client loads the group configuration settings.

Users are signed in and use desk phones for calls

1. Users sign out.
2. Users sign in and then the client notifies the users about the change to their configuration settings.
3. Users sign out.
4. Users sign in and then the client loads the group configuration settings.

If users select the option to use software phones for calls before they sign out, the client notifies the users to sign out and then sign in again to load the group configuration settings.

Group Configuration File Names

You specify the name of the group configuration files in the **Cisco Support Field** on the CSF device configuration in Cisco Unified Communications Manager.

If you remove the name of the group configuration file in the CSF device configuration on Cisco Unified Communications Manager, the client detects the change, prompts the users to sign out, and loads the global configuration file. You can remove the name of the group configuration file in the CSF device configuration by deleting the entire `configurationFile=`*`group_configuration_file_name.xml`* string or by deleting the group configuration filename from the string.

Configuration File Requirements

- Configuration filenames are case sensitive. Use lowercase letters in the filename to prevent errors and to ensure the client can retrieve the file from the TFTP server.
- You must use utf-8 encoding for the configuration files.
- The client cannot read configuration files that do not have a valid XML structure. Ensure you check the structure of your configuration file for closing elements and that elements are nested correctly.
- Your XML can contain only valid XML character entity references. For example, use `&` instead of `&`. If your XML contains invalid characters, the client cannot parse the configuration file.

Tip Open your configuration file in Microsoft Internet Explorer to see if any characters or entities are not valid.

If Internet Explorer displays the entire XML structure, your configuration file does not contain invalid characters or entities.

If Internet Explorer displays only part of the XML structure, your configuration file most likely contains invalid characters or entities.

Specify Your TFTP Server Address

The client gets configuration files from a TFTP server. The first step in configuring the client is to specify your TFTP server address so the client can access your configuration file.

Attention If Cisco Jabber gets the `_cisco-uds` SRV record from a DNS query, it can automatically locate the user's home cluster. As a result, the client can also locate the Cisco Unified Communications Manager TFTP service.

You do not need to specify your TFTP server address if you deploy the `_cisco-uds` SRV record.

Specify Your TFTP Server on Cisco Unified Presence

If you are using Cisco Unified Communications Manager Version 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Presence. If you are using Cisco Unified Communications Manager Version 9.x, then you do not need to follow the steps below.

Procedure

Step 1 Open the **Cisco Unified Presence Administration** interface.

Step 2 Select **Application** > **Cisco Jabber** > **Settings**.

Note In some versions of Cisco Unified Presence, this path is as follows: **Application** > **Cisco Unified Personal Communicator** > **Settings**.

The **Cisco Jabber Settings** window opens.

Step 3 Locate the fields to specify TFTP servers in one of the following sections, depending on your version of Cisco Unified Presence:

- **Cisco Jabber Security Settings**
- **CUPC Global Settings**

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**
- **Backup TFTP Server**

Step 5 Select **Save**.

Specify Your TFTP Server on Cisco Unified Communications Manager IM and Presence Service

If you are using Cisco Unified Communications Manager Version 8.x, complete the steps to specify the address of your TFTP server on Cisco Unified Communications Manager IM and Presence Service. If you are using Cisco Unified Communications Manager Version 9.x, then you do not need to follow the steps below.

Procedure

Step 1 Open the **Cisco Unified CM IM and Presence Administration** interface.

Step 2 Select **Application** > **Legacy Clients** > **Settings**.
The **Legacy Client Settings** window opens.

Step 3 Locate the **Legacy Client Security Settings** section.

Step 4 Specify the IP address of your primary and backup TFTP servers in the following fields:

- **Primary TFTP Server**
- **Backup TFTP Server**
- **Backup TFTP Server**

Step 5 Select **Save**.

Specify TFTP Servers with the Cisco WebEx Administration Tool

If the client connects to the Cisco WebEx Messenger service, you specify your TFTP server address with the Cisco WebEx Administration Tool.

Procedure

Step 1 Open the Cisco WebEx Administration Tool.

Step 2 Select the **Configuration** tab.

Step 3 Select **Unified Communications** in the **Additional Services** section.
The **Unified Communications** window opens.

Step 4 Select the **Clusters** tab.

Step 5 Select the appropriate cluster from the list.
The **Edit Cluster** window opens.

Step 6 Select **Advanced Server Settings** in the **Cisco Unified Communications Manager Server Settings** section.

Step 7 Specify the IP address of your primary TFTP server in the **TFTP Server** field.

Step 8 Specify the IP address of your backup TFTP servers in the **Backup Server #1** and **Backup Server #2** fields.

Step 9 Select **Save**.
The **Edit Cluster** window closes.

Step 10 Select **Save** in the **Unified Communications** window.

Create Global Configurations

Configure the client for all users in your deployment.

Remember If your environment has multiple TFTP servers, you must ensure that the configuration file is the same on all TFTP servers.

Procedure

Step 1 Create a file named `jabber-config.xml` with any text editor.

- Use lowercase letters in the filename.
- Use utf-8 encoding.

Step 2 Define the required configuration parameters in `jabber-config.xml`.

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Step 3 Host the group configuration file on your TFTP server.

Create Group Configurations

Apply different client configurations to different sets of users.

If you provision users with CSF devices, you specify the group configuration file names in the **Cisco Support Field** field on the device configuration.

If users do not have CSF devices, set a unique configuration file name for each group during installation with the TFTP_FILE_NAME argument.

Before You Begin

The **Cisco Support Field** field does not exist on Cisco Unified Communications Manager version 8.6.x or lower. You must apply a COP file as follows:

1. Download the Cisco Jabber administration package.
2. Copy `ciscocm.addcsfsupportfield.cop` from the Cisco Jabber administration package to your file system.
3. Deploy `ciscocm.addcsfsupportfield.cop` on Cisco Unified Communications Manager.

   See the Cisco Unified Communications Manager documentation for instructions on deploying COP files.

The COP file adds the **Cisco Support Field** field to CSF devices in the **Desktop Client Settings** section on the **Phone Configuration** window.

Procedure

Step 1 Create an XML group configuration file with any text editor.
The group configuration file can have any appropriate name; for example, `jabber-groupa-config.xml`.

- Use lowercase letters in the filename.
- Use utf-8 encoding.

Step 2 Define the required configuration parameters in the group configuration file.

If the structure of your configuration file is not valid, the client cannot read the values you set. Review the XML samples in this chapter for more information.

Step 3 Specify the name of the group configuration file.

a) Open the **Cisco Unified CM Administration** interface.
b) Select **Device** > **Phone**.
c) Find and select the appropriate CSF device to which the group configuration applies.
The **Phone Configuration** window opens.
d) Navigate to **Product Specific Configuration Layout** > **Desktop Client Settings**.
e) Enter `configurationfile=`*`group_configuration_file_name.xml`* in the **Cisco Support Field** field.
For example, enter the following: `configurationfile=groupa-config.xml`

Use a semicolon to delimit multiple entries. Do not add more than one group configuration file. The client uses only the first group configuration in the **Cisco Support Field** field.
If you host the group configuration file on your TFTP server in a location other than the default directory, you must specify the path and the filename; for example, `configurationfile=/customFolder/groupa-config.xml`.

f) Select **Save**.

Step 4 Host the group configuration file on your TFTP server.

Host Configuration Files

You can host configuration files on any TFTP server. However, Cisco recommends hosting configuration files on the Cisco Unified Communications Manager TFTP server, which is the same as that where the device configuration file resides.

Procedure

Step 1 Open the **Cisco Unified OS Administration** interface on Cisco Unified Communications Manager.

Step 2 Select **Software Upgrades** > **TFTP File Management**.

Step 3 Select **Upload File**.

Step 4 Select **Browse** in the **Upload File** section.

Step 5 Select the configuration file on the file system.

Step 6 Do not specify a value in the **Directory** text box in the **Upload File** section.
You should leave an empty value in the **Directory** text box so that the configuration file resides in the default directory of the TFTP server.

Step 7 Select **Upload File**.

Restart Your TFTP Server

You must restart your TFTP server before the client can access the configuration files.

Procedure

Step 1 Open the **Cisco Unified Serviceability** interface on Cisco Unified Communications Manager.

Step 2 Select **Tools** > **Control Center - Feature Services**.

Step 3 Select **Cisco Tftp** from the **CM Services** section.

Step 4 Select **Restart**.
A window displays to prompt you to confirm the restart.

Step 5 Select **OK**.
The **Cisco Tftp Service Restart Operation was Successful** status displays.

Step 6 Select **Refresh** to ensure the **Cisco Tftp** service starts successfully.

What to Do Next

To verify that the configuration file is available on your TFTP server, open the configuration file in any browser. Typically, you can access the global configuration file at the following URL:
`http://tftp_server_address:6970/jabber-config.xml`

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.

Group Elements

The following table describes the group elements you can specify in a client configuration file:

Element	Description
Client	Contains configuration parameters for the client.
Directory	Contains configuration parameters for directory integration.
Options	Contains configuration parameters for user options.
Phone	Contains configuration parameters for phone services.
Policies	Contains configuration parameters for policies.
Presence	Contains configuration parameters for presence options.
Voicemail	Contains configuration parameters for the voicemail service.

Related Topics

Summary of Configuration Parameters, on page 16

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>
```

Summary of Configuration Parameters

The following table lists all the parameters you can include in the client configuration:

Parameter	Group Element
Forgot_Password_URL	Client
Set_Status_Away_On_Inactive	Options
Set_Status_Inactive_Timeout	Options
Set_Status_Away_On_Lock_OS	Options
StartCallWithVideo	Options
ShowContactPictures	Options
ShowOfflineContacts	Options
DeviceAuthenticationPrimaryServer	Phone
DeviceAuthenticationBackupServer	Phone
TftpServer1	Phone
TftpServer2	Phone
CtiServer1	Phone
CtiServer2	Phone
useCUCMGroupForCti	Phone
CcmcipServer1	Phone
CcmcipServer2	Phone
Meeting_Server_Address	Phone
Meeting_Server_Address_Backup	Phone
Meeting_Server_Address_Backup2	Phone
EnableDSCPPacketMarking	Phone
EnableVideo	Policies
InitialPhoneSelection	Policies

Parameter	Group Element
UserDefinedRemoteDestinations	Policies
Screen_Capture_Enabled	Policies
File_Transfer_Enabled	Policies
Disallowed_File_Transfer_Types	Policies
Meetings_Enabled	Policies
Telephony_Enabled	Policies
Voicemail_Enabled	Policies
EnableSIPURIDialling	Policies
BDIDirectoryURI	Policies
ServiceDiscoveryExcludedServices	Policies
VoiceServicesDomain	Policies
LoginResource	Presence
PresenceServerAddress	Presence
PresenceServerURL	Presence
VoiceMailService_UseCredentialsFrom	Voicemail
VVM_Mailstore_Server_0	Voicemail

Related Topics

Group Elements, on page 15
Client Parameters, on page 17
Options Parameters, on page 18
Phone Parameters, on page 20
Policies Parameters, on page 23
Presence Parameters, on page 29
Service Credentials Parameters, on page 30
Voicemail Parameters, on page 30
Integrate with Directory Sources

Client Parameters

The following table describes the parameters you can specify within the Client element:

Parameter	Value	Description
Forgot_Password_URL	URL	Specifies the URL of your web page for users to reset or retrieve forgotten passwords. In hybrid cloud-based deployments, you should use the Cisco WebEx Administration Tool to direct users to the web page to reset or retrieve forgotten passwords.

Related Topics

Summary of Configuration Parameters, on page 16

Options Parameters

The following table describes the parameters you can specify within the Options element:

Parameter	Value	Description
Set_Status_Away_On_Inactive	true false	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.
Set_Status_Inactive_Timeout	Number of minutes	Sets the amount of time, in minutes, before the availability status changes to **Away** if users are inactive. The default value is 15.
Set_Status_Away_On_Lock_OS	true false	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.

Parameter	Value	Description
StartCallWithVideo	true false	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. **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. Configure this setting on the server as follows: **Cisco Unified Presence** 1 Open the **Cisco Unified Presence Administration** interface. 2 Select **Application** > **Cisco Jabber** > **Settings**. 3 Select or clear the **Always begin calls with video muted** parameter and then select **Save**. **Cisco Unified Communications Manager version 9.x and higher** 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**.
ShowContactPictures	true false	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.

Parameter	Value	Description
ShowOfflineContacts	true false	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.

Related Topics

Summary of Configuration Parameters, on page 16

Phone Parameters

The following table describes the parameters you can specify within the Phone element:

Parameter	Value	Description
DeviceAuthenticationPrimaryServer	Hostname IP address FQDN	Specifies the address of the primary instance of Cisco Unified Communications Manager to which users authenticate in phone mode deployments. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
DeviceAuthenticationBackupServer	Hostname IP address FQDN	Specifies the address of the backup instance of Cisco Unified Communications Manager to which users authenticate in phone mode deployments. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)

Parameter	Value	Description
TftpServer1	Hostname IP address FQDN	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.
TftpServer2	Hostname IP address FQDN	Specifies the address of the secondary Cisco Unified Communications Manager TFTP service. This parameter is optional.
CtiServer1	Hostname IP address FQDN	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.
CtiServer2	Hostname IP address FQDN	Specifies the address of the secondary CTI server. This parameter is optional.

Parameter	Value	Description
useCUCMGroupForCti	true false	Specifies if the Cisco Unified CM Group handles load balancing for CTI servers. Set one of the following values: **true** The Cisco Unified CM 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 CM Group does not handle CTI load balancing.
CcmcipServer1	Hostname IP address FQDN	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 version 8. In deployments with Cisco Unified Communications Manager version 9 and higher, the client can discover the CCMCIP server if you provision the `_cisco-uds` SRV record.
CcmcipServer2	Hostname IP address FQDN	Specifies the address of the secondary CCMCIP server. This parameter is optional.

Parameter	Value	Description
Meeting_Server_Address	Cisco WebEx meetings site URL	Specifies the primary Cisco WebEx meeting site URL for users. The 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 meetings site, if the Cisco WebEx 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. This parameter is optional.
Meeting_Server_Address_Backup	Cisco WebEx meetings site URL	Specifies the secondary Cisco WebEx meeting site URL for users. This parameter is optional.
Meeting_Server_Address_Backup2	Cisco WebEx meetings site URL	Specifies the tertiary Cisco WebEx meeting site URL for users. This parameter is optional.
EnableDSCPPacketMarking	true false	Specifies if DSCP marking is applied to the packets: **true (default)** DSCP marking is enabled and the checkbox in the client is not shown. **false** DSCP marking is not made to packets and the checkbox in the client is not shown.

Related Topics

Summary of Configuration Parameters, on page 16
TFTP Server Address

Policies Parameters

Policies parameters let you control specific client functionality.

Related Topics

Summary of Configuration Parameters, on page 16

On-Premises Policies

The following table describes the parameters you can specify within the Policies element in on-premises deployments:

Parameter	Value	Description
Screen_Capture_Enabled	true false	Specifies if users can take screen captures. **true (default)** Users can take screen captures. **false** Users cannot take screen captures.
File_Transfer_Enabled	true false	Specifies if users can transfer files to each other. **true (default)** Users can transfer files to each other. **false** Users cannot transfer files to each other.
Disallowed_File_Transfer_Types	File extension	Restricts users from transferring specific file types. Set file extensions as the value, for example, `.exe`. Use a semicolon to delimit multiple file extensions, for example, `.exe;.msi;.rar;.zip`.

Common Policies

The following table describes the parameters you can specify within the Policies element in both on-premises deployments and hybrid cloud-based deployments:

Parameter	Value	Description
EnableVideo	true false	Enables or disables video capabilities. **true (default)** Users can make and receive video calls. **false** Users cannot make or receive video calls.

Parameter	Value	Description
InitialPhoneSelection	deskphone softphone	Sets the phone type for users when the client starts for the first time. Users can change their phone type after the initial start. The client then saves the user preference and uses it for subsequent 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 do not provision users with software phone devices, the client automatically selects desk phone devices.
UserDefinedRemoteDestinations	true false	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.
Meetings_Enabled	true false	Enables meetings capabilities and user interface in the client. **true (default)** Enables meetings capabilities and user interface. **false** Disables meetings capabilities and user interface.

Parameter	Value	Description
Telephony_Enabled	true false	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 you are upgrading to this release, and 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.
Voicemail_Enabled	true false	Enables voicemail capabilities and user interface in the client. **true (default)** Enables voicemail capabilities and user interface. **false** Disables voicemail capabilities and user interface.
EnableSIPURIDialling	true false	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.

Parameter	Value	Description
BDIDirectoryURI	Directory attribute	Specifies the directory attribute that holds the SIP URI for users. **On-Premises Deployments** Set one of the following as the value: • mail • msRTCSIP-PrimaryUserAddress **Cloud-Based Deployments** Set one of the following as the value: • mail • imaddress • workphone • homephone • mobilephone The mail attribute is used by default. **Important** The value you specify must match the directory URI setting for users in Cisco Unified Communications Manager or the Cisco WebEx Administration Tool.

Parameter	Value	Description

ServiceDiscoveryExcludedServices	WEBEX
	CUCM
	CUP
		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`
		CUP
		When you set this value, the client:
		• Does not look for `_cuplogin`
		• Looks for `_cisco-uds_collab-edge`
		You can specify multiple, comma-separated values to exclude multiple services. For example:
		`<ServiceDiscoveryExcludedServices>`
		`WEBEX,CUCM`
		`</ServiceDiscoveryExcludedServices>`

VoiceServicesDomain	FQDN	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 would be *voice.example.com*.

Cisco WebEx Policies

If you use the Cisco WebEx Messenger service for instant messaging and presence capabilities, you can set policies for the client through the Cisco WebEx Administration Tool. See *Using policy actions available in Cisco WebEx* for a list of available policies and descriptions.

Related Topics

Using policy actions available in Cisco WebEx
Using policy actions available in Cisco WebEx

Presence Parameters

The following table describes the parameters you can specify within the Presence element:

Parameter	Value	Description
LoginResource	multiResource wbxconnect	Controls user log in to multiple client instances. **multiResource (default)** Users can log in to multiple instances of the client at the same time. **wbxconnect** Users can log in to one instance of the client at a time. The client appends the `wbxconnect` suffix to the user's JID. Users cannot log in to any other Cisco Jabber client that uses the `wbxconnect` suffix.
PresenceServerAddress	Hostname IP address FQDN	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*)
PresenceServerURL	CAS URL	Specifies the Central Authentication Service (CAS) URL for the Cisco WebEx Messenger service. The following is an example of a URL you can set as the value: `https://loginp.webexconnect.com/cas/sso/ex_org/orgadmin.app`

Related Topics

Summary of Configuration Parameters, on page 16

Service Credentials Parameters

You can specify service credentials parameters so that users do not need to authenticate with certain services.

Voicemail Service Credentials

You can specify the following parameter to configure voicemail service credentials within the Voicemail element:

Parameter	Value	Description
VoiceMailService_UseCredentialsFrom	phone	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. You should set this parameter in hybrid cloud-based deployments only. In on-premises deployments, you should set the credentials source for voicemail services on the presence server.

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>
```

Related Topics

Summary of Configuration Parameters, on page 16
Voicemail Parameters, on page 30

Voicemail Parameters

The following table describe the voicemail service configuration parameters you can specify within the Voicemail element:

Key	Value	Description
VVM_Mailstore_Server_0	Hostname IP address FQDN	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*)

Related Topics

Summary of Configuration Parameters, on page 16
Service Credentials Parameters, on page 30