Deploy Cisco Jabber Applications

Download the Cisco Jabber Clients

If required, you can add your own Customer signature to the Jabber Installer or Cisco Dynamic Libraries by using the signing tools from the Operating System for that client.

Procedure

- Visit the Cisco Software Center to download the Cisco Jabber for Mac and Cisco Jabber for Windows clients.
- For Cisco Jabber for Android, download the app from Google Play.
- For Cisco Jabber for iPhone and iPad, download the app from the App store.

Install Cisco Jabber for Windows

Cisco Jabber for Windows provides an MSI installation package that you can use in the following ways:

Install Option	Description
Use the Command Line, on page 2	You can specify arguments in a command line window to set installation properties. Choose this option if you plan to install multiple instances.

Install Option	Description
Run the MSI Manually, on page 18	Run the MSI manually on the file system of the client workstation and then specify connection properties when you start the client. Choose this option if you plan to install a single instance for testing or evaluation purposes.
Create a Custom Installer, on page 19	Open the default installation package, specify the required installation properties, and then save a custom installation package. Choose this option if you plan to distribute an installation package with the same installation properties.
Deploy with Group Policy, on page 22	Install the client on multiple computers in the same domain.

Before You Begin

You must be logged in with local administrative rights.

Use the Command Line

Specify installation arguments in a command line window.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:
```
msiexec.exe /i CiscoJabberSetup.msi
```

Step 3 Specify command line arguments as parameter=value pairs.
```
msiexec.exe /i CiscoJabberSetup.msi argument=value
```

Step 4 Run the command to install Cisco Jabber for Windows.

Cisco Jabber for Windows for Cloud Deployment

Ensure that the command line argument UPN_DISCOVERY_ENABLED is set to `false`.

Example Installation Commands

Review examples of commands to install Cisco Jabber for Windows.

Cisco Unified Communications Manager, Release 9.x

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
`/quiet` — Specifies a silent installation.

Cisco WebEx Messenger Service

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
`/quiet` — Specifies a silent installation.

Cisco WebEx Messenger Service with SSO

```
msiexec.exe /i CiscoJabberSetup.msi /quiet CLEAR=1 AUTHENTICATOR=WEBEX
 SSO_ORG_DOMAIN=example.com
```

Where:

CLEAR=1 — Deletes any existing bootstrap file.
AUTHENTICATOR=WEBEX — Sets the Cisco WebEx Messenger service as the authenticator.
SSO_ORG_DOMAIN=example.com — Sets `example.com` as the single sign-on (SSO) domain.
`/quiet` — Specifies a silent installation.

Command Line Arguments

Review the command line arguments you can specify when you install Cisco Jabber for Windows.

Override Argument

The following table describes the parameter you must specify to override any existing bootstrap files from previous installations:

Argument	Value	Description
CLEAR	1	Specifies if the client overrides any existing bootstrap file from previous installations. The client saves the arguments and values you set during installation to a bootstrap file. The client then loads settings from the bootstrap file at startup.

If you specify CLEAR, the following occurs during installation:

1. The client deletes any existing bootstrap file.
2. The client creates a new bootstrap file.

If you do not specify CLEAR, the client checks for existing bootstrap files during installation.

- If no bootstrap file exists, the client creates a bootstrap file during installation.
- If a bootstrap file exists, the client does not override that bootstrap file and preserves the existing settings.

Note If you are reinstalling Cisco Jabber for Windows, you should consider the following:

- The client does not preserve settings from existing bootstrap files. If you specify CLEAR, you must also specify all other installation arguments as appropriate.
- The client does not save your installation arguments to an existing bootstrap file. If you want to change the values for installation arguments, or specify additional installation arguments, you must specify CLEAR to override the existing settings.

To override existing bootstrap files, specify CLEAR in the command line as follows:

```
msiexec.exe /i CiscoJabberSetup.msi CLEAR=1
```

Mode Type Argument

The following table describes the command line argument with which you specify the product mode:

Argument	Value	Description
PRODUCT_MODE	Phone_Mode	Specifies the product mode for the client. You can set the following value: • Phone_Mode — Cisco Unified Communications Manager is the authenticator. Choose this value to provision users with audio devices as base functionality.

When to Set the Product Mode

In phone mode deployments Cisco Unified Communications Manager is the authenticator. When the client gets the authenticator, it determines the product mode is phone mode. However, because the client always starts in the default product mode on the initial launch, users must restart the client to enter phone mode after sign in.

- Cisco Unified Communications Manager, Release 9.x and Later — You should not set PRODUCT_MODE during installation. The client gets the authenticator from the service profile. After the user signs in, the client requires a restart to enter phone mode.

Change Product Modes

To change the product mode, you must change the authenticator for the client. The client can then determine the product mode from the authenticator.

The method for changing from one product mode to another after installation, depends on your deployment.

Note In all deployments, the user can manually set the authenticator in the Advanced settings window.

In this case, you must instruct the user to change the authenticator in the Advanced settings window to change the product mode. You cannot override the manual settings, even if you uninstall and then reinstall the client.

Change Product Modes with Cisco Unified Communications Manager Version 9.x and Later

To change product modes with Cisco Unified Communications Manager version 9.x and later, you change the authenticator in the service profile.

Procedure

Step 1 Change the authenticator in the service profiles for the appropriate users.

Change Default Mode > Phone Mode

Do not provision users with an IM and Presence service.

If the service profile does not contain an IM and presence service configuration, the authenticator is Cisco Unified Communications Manager.

Change Phone Mode > Default Mode

Provision users with an IM and Presence service.

If you set the value of the **Product type** field in the IM and Presence profile to:

- **Unified CM (IM and Presence)** the authenticator is Cisco Unified Communications Manager IM and Presence Service.
- **WebEx (IM and Presence)** the authenticator is the Cisco WebEx Messenger service.

Step 2 Instruct users to sign out and then sign in again.

When users sign in to the client, it retrieves the changes in the service profile and signs the user in to the authenticator. The client then determines the product mode and prompts the user to restart the client.

After the user restarts the client, the product mode change is complete.

Authentication Arguments

The following table describe the command line arguments you can set to specify the source of authentication:

Argument	Value	Description
AUTHENTICATOR	CUP CUCM WEBEX	Specifies the source of authentication for the client. This value is used if Service Discovery fails. Set one of the following as the value: • CUP—Cisco Unified Communications Manager IM and Presence Service. On-premises deployments in the default product mode. The default product mode can be either full UC or IM only. • CUCM—Cisco Unified Communications Manager. On-premises deployments in phone mode. • WEBEX—Cisco WebEx Messenger Service. Cloud-based or hybrid cloud-based deployments. In on-premises deployments with Cisco Unified Communications Manager version 9.x and later, you should deploy the `_cisco-uds` SRV record. The client can then automatically determine the authenticator.
CUP_ADDRESS	IP address Hostname FQDN	Specifies the address of Cisco Unified Communications Manager IM and Presence Service. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*)
TFTP	IP address Hostname FQDN	Specifies the address of your TFTP server. Set one of the following as the value: • Hostname (*hostname*) • IP address (*123.45.254.1*) • FQDN (*hostname.domain.com*) You should specify this argument if you set Cisco Unified Communications Manager as the authenticator. If you deploy: • In phone mode—you should specify the address of the TFTP server that hosts the client configuration. • In default mode—you can specify the address of the Cisco Unified Communications Manager TFTP service that hosts the device configuration.

Argument	Value	Description
CTI	IP address Hostname FQDN	Sets the address of your CTI server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • Users have desk phone devices and require a CTI server.
CCMCIP	IP address Hostname FQDN	Sets the address of your CCMCIP server. Specify this argument if: • You set Cisco Unified Communications Manager as the authenticator. • The address of your CCMCIP server is not the same as the TFTP server address. The client can locate the CCMCIP server with the TFTP server address if both addresses are the same. 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 *Feature and Services* guide for your Cisco Unified Communications Manager release.
SERVICES_DOMAIN	Domain	Sets the value of the domain where the DNS SRV records for Service Discovery reside. This argument can be set to a domain where no DNS SRV records reside if you want the client to use installer settings or manual configuration for this information. If this argument is not specified and Service Discovery fails, the user will be prompted for services domain information.

Argument	Value	Description
VOICE_SERVICES_DOMAIN	Domain	In Hybrid Deployments the domain required to discover Webex via CAS lookup may be a different domain than where the DNS records are deployed. If this is the case then set the SERVICES_DOMAIN to be the domain used for Webex discovery (or let the user enter an email address) and set the VOICE_SERVICES_DOMAIN to be the domain where DNS records are deployed. If this setting is specified, the client will use the value of VOICE_SERVICES_DOMAIN to lookup the following DNS records for the purposes of Service Discovery and Edge Detection: • `_cisco-uds` • `_cuplogin` • `_collab-edge` This setting is optional and if not specified, the DNS records are queried on the Services Domain which is obtained from the SERVICES_DOMAIN, email address input by the user, or cached user configuration.
EXCLUDED_SERVICES	One or more of: • WEBEX • CUCM	Lists the services that you want Jabber to exclude from Service Discovery. For example, you may have done a trial with WebEx which means that your company domain is registered on WebEx, but you do not want Jabber users to authenticate using WebEx. You want Jabber to authenticate with CUCM server. In this case set: • EXCLUDED_SERVICES=WEBEX Possible values are CUCM, WEBEX. If you exclude all services, you need to use manual configuration or bootstrap configuration to configure the Jabber client.

Argument	Value	Description
UPN_DISCOVERY_ENABLED	true false	Allows you to define whether the client uses the User Principal Name (UPN) of a Windows session to get the User ID and domain for a user when discovering services. • true (default)—The UPN is used to find the User ID and the domain of the user, which is used during service discovery. Only the user discovered from UPN can log in to the client. • false—The UPN is not used to find the User ID and domain of the user. The user is prompted to enter credentials to find the domain for service discovery. Example installation command: `msiexec.exe /i CiscoJabberSetup.msi /quiet UPN_DISCOVERY_ENABLED=false`

TFTP Server Address

Cisco Jabber for Windows retrieves two different configuration files from the TFTP server:

- Client configuration files that you create.
- Device configuration files that reside on the Cisco Unified Communications Manager TFTP service when you provision users with devices.

To minimize effort, you should host your client configuration files on the Cisco Unified Communications Manager TFTP service. You then have only one TFTP server address for all configuration files and can specify that address as required.

You can, however, host your client configuration on a different TFTP server to the one that contains the device configuration. In this case, you have two different TFTP server addresses, one address for the TFTP server that hosts device configuration and another address for the TFTP server that hosts client configuration files.

Default Deployments

This section describes how you should handle two different TFTP server addresses in deployments that have a presence server.

You should do the following:

1. Specify the address of the TFTP server that hosts the client configuration on the presence server.
2. During installation, specify the address of the Cisco Unified Communications Manager TFTP service with the TFTP argument.

When the client starts for the first time, it:

1. Retrieves the address of the Cisco Unified Communications Manager TFTP service from the bootstrap file.
2. Gets device configuration from the Cisco Unified Communications Manager TFTP service.

3 Connects to the presence server.

4 Retrieves the address of the TFTP service that hosts the client configuration from the presence server.

5 Gets client configuration from the TFTP server.

Phone Mode Deployments

This section describes how you should handle two different TFTP server addresses in phone mode deployments.

You should do the following:

1 During installation, specify the address of the TFTP server that hosts the client configuration with the TFTP argument.

2 Specify the address of the TFTP server that hosts the device configuration in your client configuration file with the following parameter: TftpServer1.

3 Host the client configuration file on the TFTP server.

When the client starts for the first time, it:

1 Retrieves the address of the TFTP server from the bootstrap file.

2 Gets client configuration from the TFTP server.

3 Retrieves the address of the Cisco Unified Communications Manager TFTP service from the client configuration.

4 Gets device configuration from the Cisco Unified Communications Manager TFTP service.

Common Installation Arguments

The following table describes command line arguments that are common to all deployments:

Argument	Value	Description
LANGUAGE	LCID in decimal	Defines the Locale ID (LCID), in decimal, of the language that Cisco Jabber for Windows uses. The value must be an LCID in decimal that corresponds to a supported language. For example, you can specify one of the following: • 1033 specifies English. • 1036 specifies French. See the *LCID for Languages* topic for a full list of the languages that you can specify. This argument is optional. If you do not specify a value, Cisco Jabber for Windows uses the regional language for the current user as the default. From Release 11.1(1) onwards, if you do not specify a value, Cisco Jabber for Windows checks the value for the UseSystemLanguage parameter. If the UseSystemLanguage parameter is set to true, the same language is used as for the operating system. If the UseSystemLanguage parameter is to set to false or not defined, then the client uses the regional language for the current user as the default. The regional language is set at **Control Panel** > **Region and Language** > **Change the date, time, or number format** > **Formats tab** > **Format dropdown**.
FORGOT_PASSWORD_URL	URL	Specifies the URL where users can reset lost or forgotten passwords. This argument is optional but recommended. **Note** In cloud-based deployments, you can specify a forgot password URL using the Cisco WebEx Administration Tool. However, the client cannot retrieve that forgot password URL until users sign in.

Argument	Value	Description
AUTOMATIC_SIGN_IN	true false	Applies to Release 11.1(1) onwards. Specifies whether the **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • true—The **Sign me in when Cisco Jabber starts** check box is checked when the user installs the client. • false (default)—The **Sign me in when Cisco Jabber starts** check box is not checked when the user installs the client.
TFTP_FILE_NAME	Filename	Specifies the unique name of a group configuration file. You can specify either an unqualified or fully qualified filename as the value. The filename you specify as the value for this argument takes priority over any other configuration file on your TFTP server. This argument is optional. **Remember** You can specify group configuration files in the **Cisco Support Field** on the CSF device configuration on Cisco Unified Communications Manager.

Argument	Value	Description
LOGIN_RESOURCE	WBX MUT	Controls user sign in to multiple client instances. By default, users can sign in to multiple instances of Cisco Jabber at the same time. Set one of the following values to change the default behavior: • WBX—Users can sign in to one instance of Cisco Jabber for Windows at a time. Cisco Jabber for Windows appends the `wbxconnect` suffix to the user's JID. Users cannot sign in to any other Cisco Jabber client that uses the `wbxconnect` suffix. • MUT—Users can sign in to one instance of Cisco Jabber for Windows at a time, but can sign in to other Cisco Jabber clients at the same time. Each instance of Cisco Jabber for Windows appends the user's JID with a unique suffix.
LOG_DIRECTORY	Absolute path on the local filesystem	Defines the directory where the client writes log files. Use quotation marks to escape space characters in the path, as in the following example: `"C:\my_directory\Log Directory"` The path you specify must not contain Windows invalid characters. The default value is `%USER_PROFILE%\AppData\Local\Cisco\Unified Communications\Jabber\CSF\Logs`
CLICK2X	DISABLE	Disables click-to-x functionality with Cisco Jabber. If you specify this argument during installation, the client does not register as a handler for click-to-x functionality with the operating system. This argument prevents the client from writing to the Microsoft Windows registry during installation. You must re-install the client and omit this argument to enable click-to-x functionality with the client after installation.

Argument	Value	Description
ENABLE_PRT	true false	• true (default)—The **Report a problem** menu item is enabled in the **Help** menu in the client. • false—The Jabber menu item option **Report a problem** is removed from the **Help** menu in the client. If you set the argument to false, 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.
ENABLE_PRT_ENCRYPTION	true false	Enables problem report encryption. You must configure this argument with the PRT_CERTIFICATE_NAME argument. • true—PRT files sent by Jabber clients are encrypted. • false (default)—PRT files sent by Jabber clients are not encrypted. PRT encryption requires a public/private key pair to encrypt and decrypt the Cisco Jabber problem report.
PRT_CERTIFICATE_NAME	Certificate name	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 Jabber Problem reports. You must configure this argument with the ENABLE_PRT_ENCRYPTION argument.

Argument	Value	Description
INVALID_CERTIFICATE_BEHAVIOR	RejectAndNotify PromptPerSession	Specifies the client behavior for invalid certificates. • RejectAndNotify—A warning dialog displays and the client doesn't load. • PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate. For invalid certificates in FIPS mode, this argument is ignored, the client displays a warning message and doesn't load.
Telemetry_Enabled	true false	Specifies whether analytics data is gathered. The default value is true. To improve your experience and product performance, Cisco Jabber may collect and send non-personally identifiable usage and performance data to Cisco. The aggregated data is used by Cisco to understand trends in how Jabber clients are being used and how they are performing. Full details on what analytics data Cisco Jabber does and does not collect can be found in the Cisco Jabber Supplement to Cisco's On-Line Privacy Policy at http://www.cisco.com/web/siteassets/legal/privacy_02Jun10.html.
LOCATION_MODE	ENABLED DISABLED ENABLEDNOPROMPT	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.

Argument	Value	Description
FIPS_MODE	true false	Specifies whether the Cisco Jabber is in FIPS mode. Cisco Jabber can be in FIPS mode on an operating system that is not FIPS enabled. Only connections with non-Window's APIs are in FIPS mode. If you don't include this setting, Cisco Jabber will determine the FIPS mode from the operating system.
ENABLE_DPI_AWARE	true false	Enables DPI awareness. DPI awareness enables Cisco Jabber to automatically adjust the display of text and images to suit different screen sizes. • true (default)—DPI awareness is enabled. • false—DPI awareness is not enabled. DPI awareness is enabled by default. To disable DPI awareness, use the following command: `msiexec.exe /i CiscoJabberSetup.msi CLEAR=1 ENABLE_DPI_AWARE=false`

SSO Arguments

This section describes the command line arguments you can use to deploy Cisco Jabber for Windows with single sign on (SSO) capabilities.

Cloud-Based SSO Arguments

The arguments in the following table apply to cloud-based deployments only:

Argument	Value	Description
SSO_ORG_DOMAIN	Domain name	Specifies the domain name for the Cisco WebEx Org that contains the URL for the SSO service. Cisco Jabber for Windows uses this argument to retrieve the URL of the SSO service from the Org. When Cisco Jabber for Windows gets the SSO service URL, it can request login tokens to authenticate with Cisco WebEx Messenger. **Note** You specify the URL for the SSO service as the value of the Customer SSO Service Login URL in the Cisco WebEx Administration Tool.

LCID for Languages

The following table lists the Locale Identifier (LCID) or Language Identifier (LangID) for the languages that the Cisco Jabber clients support.

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Arabic - Saudi Arabia	X		X	1025
Bulgarian - Bulgaria	X	X		1026
Catalan - Spain	X	X		1027
Chinese (Simplified) - China	X	X	X	2052
Chinese (Traditional) - Taiwan	X	X	X	1028
Croatian - Croatia	X	X		1050
Czech - Czech Republic	X	X		1029
Danish - Denmark	X	X	X	1030
Dutch - Netherlands	X	X	X	1043
English - United States	X	X	X	1033
Finnish - Finland	X	X		1035
French - France	X	X	X	1036
German - Germany	X	X	X	1031
Greek - Greece	X	X		1032
Hebrew - Israel	X			1037
Hungarian - Hungary	X	X		1038
Italian - Italy	X	X	X	1040

Supported Languages	Cisco Jabber for Windows	Cisco Jabber for Mac	Cisco Jabber for Android, Cisco Jabber for iPhone and iPad	LCID/LangID
Japanese - Japan	X	X	X	1041
Korean - Korea	X	X	X	1042
Norwegian - Norway	X	X		2068
Polish - Poland	X	X		1045
Portuguese - Brazil	X	X	X	1046
Portuguese - Portugal	X	X		2070
Romanian - Romania	X	X		1048
Russian - Russia	X	X	X	1049
Serbian	X	X		1050
Slovak - Slovakian	X	X		1051
Slovenian -Slovenia	X	X		1060
Spanish - Spain (Modern Sort)	X	X	X	3082
Swedish - Sweden	X	X	X	5149
Thai - Thailand	X	X		1054
Turkish	X	X		1055

Run the MSI Manually

You can run the installation program manually to install a single instance of the client and specify connection settings in the Advanced settings window.

Procedure

Step 1 Launch `CiscoJabberSetup.msi`.

The installation program opens a window to guide you through the installation process.

Step 2 Follow the steps to complete the installation process.

Step 3 Start Cisco Jabber for Windows.

Step 4 Select **Manual setup and sign in**.
The Advanced settings window opens.

Step 5 Specify values for the connection settings properties.

Step 6 Select **Save**.

Create a Custom Installer

You can transform the default installation package to create a custom installer.

Note You use Microsoft Orca to create custom installers. Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and .NET Framework 4.

Download and install Microsoft Windows SDK for Windows 7 and .NET Framework 4 from the Microsoft website.

Procedure

	Command or Action	Purpose
Step 1	Get the Default Transform File, on page 19	You must have the default transform file to modify the installation package with Microsoft Orca.
Step 2	Create Custom Transform Files, on page 20	Transform files contain installation properties that you apply to the installer.
Step 3	Transform the Installer, on page 20	Apply a transform file to customize the installer.

Get the Default Transform File

You must have the default transform file to modify the installation package with Microsoft Orca.

Procedure

Step 1 Download the Cisco Jabber administration package from Software Download page.

Step 2 Copy `CiscoJabberProperties.msi` from the Cisco Jabber administration package to your file system.

What to Do Next

Create Custom Transform Files, on page 20

Create Custom Transform Files

To create a custom installer, you use a transform file. Transform files contain installation properties that you apply to the installer.

The default transform file lets you specify values for properties when you transform the installer. You should use the default transform file if you are creating one custom installer.

You can optionally create custom transform files. You specify values for properties in a custom transform file and then apply it to the installer.

Create custom transform files if you require more than one custom installer with different property values. For example, create one transform file that sets the default language to French and another transform file that sets the default language to Spanish. You can then apply each transform file to the installation package separately. The result is that you create two installers, one for each language.

Before You Begin

Get the Default Transform File, on page 19

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` and then apply `CiscoJabberProperties.msi`.

Step 3 Specify values for the appropriate installer properties.

Step 4 Generate and save the transform file.

a) Select **Transform** > **Generate Transform**.

b) Select a location on your file system to save the transform file.

c) Specify a name for the transform file and select **Save**.

The transform file you created is saved as *`file_name`*`.mst`. You can apply this transform file to modify the properties of `CiscoJabberSetup.msi`.

What to Do Next

Transform the Installer, on page 20

Transform the Installer

Apply a transform file to customize the installer.

Note Applying transform files will alter the digital signature of `CiscoJabberSetup.msi`. Attempts to modify or rename `CiscoJabberSetup.msi` will remove the signature entirely.

Before You Begin

Create Custom Transform Files, on page 20

Procedure

Step 1 Start Microsoft Orca.

Step 2 Open `CiscoJabberSetup.msi` in Microsoft Orca.

a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

The installation package opens in Microsoft Orca. The list of tables for the installer opens in the **Tables** pane.

Step 3 Remove all language codes except for 1033 (English).

Restriction You must remove all language codes from the custom installer except for 1033 (English).

Microsoft Orca does not retain any language files in custom installers except for the default, which is 1033. If you do not remove all language codes from the custom installer, you cannot run the installer on any operating system where the language is other than English.

a) Select **View** > **Summary Information**.
The **Edit Summary Information** window displays.
b) Locate the **Languages** field.
c) Delete all language codes except for 1033.
d) Select **OK**.

English is set as the language for your custom installer.

Step 4 Apply a transform file.

a) Select **Transform** > **Apply Transform**.
b) Browse to the location of the transform file on your file system.
c) Select the transform file and then select **Open**.

Step 5 Select **Property** from the list of tables in the **Tables** pane.
The list of properties for `CiscoJabberSetup.msi` opens in the right panel of the application window.

Step 6 Specify values for the properties you require.

Tip Values are case sensitive. Ensure the value you enter matches the value in this document.

Tip Set the value of the CLEAR property to `1` to override any existing bootstrap file from previous installations. If you do not override existing bootstrap files, the values you set in the custom installer do not take effect.

Step 7 Remove any properties that you do not require.
It is essential to remove any properties that are not being set, otherwise the properties being set will not take effect. Remove each property that is not needed one at a time.

a) Right-click the property you want to remove.
b) Select **Drop Row**.
c) Select **OK** when Microsoft Orca prompts you to continue.

Step 8 Enable your custom installer to save embedded streams.

a) Select **Tools** > **Options**.

b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 9 Save your custom installer.

a) Select **File** > **Save Transformed As**.
b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

Installer Properties

The following are the properties you can modify in a custom installer:

- CLEAR
- PRODUCT_MODE
- AUTHENTICATOR
- CUP_ADDRESS
- TFTP
- CTI
- CCMCIP
- LANGUAGE
- TFTP_FILE_NAME
- FORGOT_PASSWORD_URL
- SSO_ORG_DOMAIN
- LOGIN_RESOURCE
- LOG_DIRECTORY
- CLICK2X
- SERVICES_DOMAIN

These properties correspond to the installation arguments and have the same values.

Deploy with Group Policy

Install Cisco Jabber for Windows with Group Policy using the Microsoft Group Policy Management Console (GPMC) on Microsoft Windows Server.

Note To install Cisco Jabber for Windows with Group Policy, all computers or users to which you plan to deploy Cisco Jabber for Windows must be in the same domain.

Procedure

	Command or Action	Purpose
Step 1	Set a Language Code, on page 23	You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.
Step 2	Deploy the Client with Group Policy, on page 24	Deploy Cisco Jabber for Windows with Group Policy.

Set a Language Code

Altering the installation language is not necessary in Group Policy deployment scenarios where the exact MSI file provided by Cisco will be used. The installation language will be determined from the Windows User Locale (Format) in these situations. You must use this procedure and set the Language field to 1033 only if the MSI is to be modified by Orca in any way.

Procedure

Step 1 Start Microsoft Orca.
Microsoft Orca is available as part of the Microsoft Windows SDK for Windows 7 and ,NET Framework 4 that you can download from the Microsoft website.

Step 2 Open `CiscoJabberSetup.msi`.
a) Select **File** > **Open**.
b) Browse to the location of `CiscoJabberSetup.msi` on your file system.
c) Select `CiscoJabberSetup.msi` and then select **Open**.

Step 3 Select **View** > **Summary Information**.

Step 4 Locate the **Languages** field.

Step 5 Set the **Languages** field to 1033.

Step 6 Select **OK**.

Step 7 Enable your custom installer to save embedded streams.
a) Select **Tools** > **Options**.
b) Select the **Database** tab.
c) Select **Copy embedded streams during 'Save As'**.
d) Select **Apply** and then **OK**.

Step 8 Save your custom installer.
a) Select **File** > **Save Transformed As**.

b) Select a location on your file system to save the installer.
c) Specify a name for the installer and then select **Save**.

What to Do Next

Deploy the Client with Group Policy, on page 24

Deploy the Client with Group Policy

Complete the steps in this task to deploy Cisco Jabber for Windows with Group Policy.

Before You Begin

Set a Language Code, on page 23

Procedure

Step 1 Copy the installation package to a software distribution point for deployment.
All computers or users to which you plan to deploy Cisco Jabber for Windows must be able to access the installation package on the distribution point.

Step 2 Select **Start** > **Run** and then enter the following command:
`GPMC.msc`

The **Group Policy Management** console opens.

Step 3 Create a new group policy object.

a) Right-click on the appropriate domain in the left pane.
b) Select **Create a GPO in this Domain, and Link it here**.
The **New GPO** window opens.
c) Enter a name for the group policy object in the **Name** field.
d) Leave the default value or select an appropriate option from the **Source Starter GPO** drop-down list and then select **OK**.
The new group policy displays in the list of group policies for the domain.

Step 4 Set the scope of your deployment.

a) Select the group policy object under the domain in the left pane.
The group policy object displays in the right pane.
b) Select **Add** in the **Security Filtering** section of the **Scope** tab.
The **Select User, Computer, or Group** window opens.
c) Specify the computers and users to which you want to deploy Cisco Jabber for Windows.

Step 5 Specify the installation package.

a) Right-click the group policy object in the left pane and then select **Edit**.
The **Group Policy Management Editor** opens.
b) Select **Computer Configuration** and then select **Policies** > **Software Settings**.
c) Right-click **Software Installation** and then select **New** > **Package**.

d) Enter the location of the installation package next to **File Name**; for example, `\\server\software_distribution`.

Important You must enter a Uniform Naming Convention (UNC) path as the location of the installation package. If you do not enter a UNC path, Group Policy cannot deploy Cisco Jabber for Windows.

e) Select the installation package and then select **Open**.

f) In the **Deploy Software** dialog box, select **Assigned** and then **OK**.

Group Policy installs Cisco Jabber for Windows on each computer the next time each computer starts.

Cisco Media Services Interface

Cisco Jabber for Windows supports Cisco Media Services Interface version 4.1.2 for Microsoft Windows 7 and later.

Cisco Jabber for Mac supports Cisco Media Services Interface version 4.0.2 or later.

Desk Phone Video Capabilities

You must install Cisco Media Services Interface to enable desk phone video capabilities. Cisco Media Services Interface provides a driver that enables Cisco Jabber for Windows to do the following:

- Discover the desk phone device.
- Establish and maintain a connection to the desk phone device using the CAST protocol.

Install Cisco Media Services Interface

Procedure

Step 1 Download the Cisco Media Services Interface installation program from the download site on cisco.com.

Step 2 Install Cisco Media Services Interface on each computer on which you install Cisco Jabber.
See the appropriate Cisco Medianet documentation for installing Cisco Media Services Interface.

Uninstall Cisco Jabber for Windows

You can uninstall Cisco Jabber for Windows using either the command line or the Microsoft Windows control panel. This document describes how to uninstall Cisco Jabber for Windows using the command line.

Use the Installer

If the installer is available on the file system, use it to remove Cisco Jabber for Windows.

Procedure

Step 1 Open a command line window.

Step 2 Enter the following command:
`msiexec.exe /x path_to_CiscoJabberSetup.msi`

For example,
`msiexec.exe /x C:\Windows\Installer\CiscoJabberSetup.msi /quiet`
Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Use the Product Code

If the installer is not available on the file system, use the product code to remove Cisco Jabber for Windows.

Procedure

Step 1 Find the product code.

a) Open the Microsoft Windows registry editor.
b) Locate the following registry key: `HKEY_CLASSES_ROOT\Installer\Products`
c) Select **Edit** > **Find**.
d) Enter Cisco Jabber in the **Find what** text box in the **Find** window and select **Find Next**.
e) Find the value of the **ProductIcon** key.
The product code is the value of the **ProductIcon** key, for example, `C:\Windows\Installer\{product_code}\ARPPRODUCTICON.exe`.

Note The product code changes with each version of Cisco Jabber for Windows.

Step 2 Open a command line window.

Step 3 Enter the following command:
`msiexec.exe /x product_code`

For example,
`msiexec.exe /x 45992224-D2DE-49BB-B085-6524845321C7 /quiet`
Where `/quiet` specifies a silent uninstall.

The command removes Cisco Jabber for Windows from the computer.

Install Cisco Jabber for Mac

URL Configuration for Cisco Jabber for Mac

To enable users to launch Cisco Jabber without having to manually enter service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
    - WEBEX—When you set this value, the client:
        - Does not perform CAS lookup
        - Looks for:
            - `_cisco-uds`
            - `_cuplogin`
            - `_collab-edge`
    - CUCM—When you set this value, the client:
        - Does not look for `_cisco-uds`
        - Looks for:
            - `_cuplogin`
            - `_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.

If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.

- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF
- EnablePRTEncryption—Optional. Specifies that the PRT file is encrypted. Applies to Cisco Jabber for Mac.
  - true
  - false
- PRTCertificateName—Optional. Specifies the name of the certificate. Applies to Cisco Jabber for Mac.
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.
  - RejectAndNotify—A warning dialog displays and the client doesn't load.
  - PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive. When you create the configuration URL, you must use the following capitlization:

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `EnablePRTEncryption`
- `PRTCertificateName`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Install Cisco Jabber Mobile Clients

Procedure

Step 1 To install Cisco Jabber for Android, download the app from Google Play from your mobile device.

Step 2 To install Cisco Jabber for iPhone and iPad, download the app from the App Store from your mobile device.

URL Configuration for Cisco Jabber for Android, iPhone, and iPad

To enable users to launch Cisco Jabber without having to manually enter service discovery information, create and distribute a configuration URL to users.

You can provide a configuration URL link to users by emailing the link to the user directly, or by posting the link to a website.

You can include and specify the following parameters in the URL:

- ServicesDomain—Required. Every configuration URL must include the domain of the IM and presence server that Cisco Jabber needs for service discovery.
- VoiceServiceDomain—Required only if you deploy a hybrid cloud-based architecture where the domain of the IM and presence server differs from the domain of the voice server. Set this parameter to ensure that Cisco Jabber can discover voice services.
- ServiceDiscoveryExcludedServices—Optional. You can exclude any of the following services from the service discovery process:
  - WEBEX—When you set this value, the client:
    - Does not perform CAS lookup
    - Looks for:
      - `_cisco-uds`
      - `_cuplogin`
      - `_collab-edge`
  - CUCM—When you set this value, the client:
    - Does not look for `_cisco-uds`
    - Looks for:
      - `_cuplogin`
      - `_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.

  If you exclude all three services, the client does not perform service discovery and prompts the user to manually enter connection settings.
- ServicesDomainSsoEmailPrompt—Optional. Specifies whether the user is shown the email prompt for the purposes of determining their home cluster.
  - ON
  - OFF
- InvalidCertificateBehavior—Optional. Specifies the client behavior for invalid certificates.

- RejectAndNotify—A warning dialog displays and the client doesn't load.
- PromptPerSession—A warning dialog displays and the user can accept or reject the invalid certificate.

- PRTCertificateUrl—Specifies the name of a certificate with a public key in the trusted root certificate store. Applies to Cisco Jabber mobile clients.
- Telephony_Enabled—Specifies whether the user has phone capability or not. The default is true.
  - True
  - False
- ForceLaunchBrowser—Used to force user to use the external browser. Applies to Cisco Jabber mobile clients.
  - True
  - False

Note ForceLaunchBrowser is used for client certificate deployments and for devices with Android OS below 5.0.

Create the configuration URL in the following format:

```
ciscojabber://provision?ServicesDomain=<domain_for_service_discover>
&VoiceServicesDomain=<domain_for_voice_services>
&ServiceDiscoveryExcludedServices=<services_to_exclude_from_service_discover>
&ServicesDomainSsoEmailPrompt=<ON/OFF>
```

Note The parameters are case sensitive. When you create the configuration URL, use the following capitalization:

- `ServicesDomain`
- `VoiceServicesDomain`
- `ServiceDiscoveryExcludedServices`
- `ServicesDomainSsoEmailPrompt`
- `PRTCertificateURL`
- `InvalidCertificateBehavior`
- `Telephony_Enabled`
- `ForceLaunchBrowser`

Examples

- `ciscojabber://provision?ServicesDomain=cisco.com`

- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com`
- `ciscojabber://provision?ServicesDomain=service_domain &VoiceServicesDomain=voiceservice_domain&ServiceDiscoveryExcludedServices=WEBEX`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP`
- `ciscojabber://provision?ServicesDomain=cisco.com &VoiceServicesDomain=alphauk.cisco.com&ServiceDiscoveryExcludedServices=CUCM,CUP &ServicesDomainSsoEmailPrompt=OFF`

Mobile Configuration Using Enterprise Mobility Management

Before using Enterprise Mobility Management (EMM), ensure:

- The EMM vendor supports Android for Work or Apple Managed App Configuration.
- Android devices OS is 5.0 or later

To allow users to launch Cisco Jabber for Android or Cisco Jabber for iPhone and iPad, you can configure Cisco Jabber using Enterprise Mobility Management (EMM).

For more information on setting up EMM, refer to the instructions for administrators provided by the EMM provider.

If you want Jabber to run only on managed devices, then you can deploy certificate-based authentication, and enroll the client certificate through EMM.