Configure Directory Integration

Client Configuration for Directory Integration

You can configure directory integration through service profiles using Cisco Unified Communications Manager release 9 or later or with the configuration file. Use this section to learn how to configure the client for directory integration.

When both a service profile and a configuration file are present, the following table describes which parameter value takes precedence.

Service Profile	Configuration File	Which Parameter Value Takes Precedence?
Parameter value is set	Parameter value is set	Service profile
Parameter value is set	Parameter value is blank	Service profile
Parameter value is blank	Parameter value is set	Configuration file
Parameter value is blank	Parameter value is blank	Service profile blank (default) value

Note Cisco Unified Presence, Release 8.x profiles cannot be used for directory integration.

When to Configure Directory Integration

Note Install Cisco Jabber for Windows on a workstation that is registered to an Active Directory domain. In this environment, you do not need to configure Cisco Jabber for Windows to connect to the directory. The client automatically discovers the directory and connects to a Global Catalog server in that domain.

Configure Cisco Jabber to connect to a directory if you plan to use one of the following as the contact source:

- Domain Controller
- Cisco Unified Communications Manager User Data Service
- OpenLDAP
- Active Directory Lightweight Directory Service
- Active Directory Application Mode

You can optionally configure directory integration to:

- Change the default attribute mappings.
- Adjust directory query settings.
- Specify how the client retrieves contact photos.
- Perform intradomain federation.

Configure Directory Integration in a Service Profile

With Cisco Unified Communications Manager version 9 and higher, you can provision users with service profiles and deploy the `_cisco-uds` SRV record on your internal domain name server.

The client can then automatically discover Cisco Unified Communications Manager and retrieve the service profile to get directory integration configuration.

To set up service discovery to support service profiles, you must:

- Deploy the `_cisco-uds` SRV record on your internal domain name server.
- Ensure that the client can resolve the domain name server address.
- Ensure that the client can resolve the hostname of Cisco Unified Communications Manager.
- Ensure that the client can resolve the fully qualified domain name (FQDN) for the Cisco Unified Communications Manager.

Cisco Jabber now supports Cisco Unified Communications Manager User Data Service (UDS). In addition to being able to deploy Cisco Jabber using LDAP to connect to Active Directory, Jabber can now alternatively be deployed with Cisco Unified Communications Manager User Data Services contact lookup service. Server scaling must be considered when using the UDS server. A Cisco Unified Communication node can support UDS contact service connections for 50% of the maximum device registrations supported by the server.

To configure directory integration in a service profile, do the following:

Procedure

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

Step 2 Add a directory service.

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

b) Select **Add New**.
The **UC Service Configuration** window opens.

c) Select **Directory** from the **UC Service Type** menu and then select **Next**.

d) Set all appropriate values for the directory service and then select **Save**.

Step 3 Apply the directory service to a service profile.

a) Select **User Management** > **User Settings** > **Service Profile**.
The **Find and List Service Profiles** window opens.

b) Select **Add New**.
The **Service Profile Configuration** window opens.

c) Add the directory services to the directory profile.

d) Select **Save**.

When both the directory profile and `jabber-config.xml` file are used at the same time, the configuration in the directory profile have the higher priority and will be used except manual sign-in and service discovery.

To make it work consistently, it is highly recommended that **Username** and **Password** in both directory profile and `jabber-config.xml` are exactly the same.

Directory Profile Parameters

The following table lists the configuration parameters you need to set in the directory profile:

Directory Service Configuration	Description
Primary server	Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.
Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.

Directory Service Configuration	Description
Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. You should use this parameter only in deployments where you cannot authenticate with the directory server using Microsoft Windows credentials. If you must use this parameter, you should use only a well-known or public set of credentials. The credentials should also be linked to an account that has read-only permissions.
Search Base 1	Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree. You can specify the value of up to three search bases in your OU to override the default behavior. Active Directory does not typically require a search base. You should specify search bases for Active Directory only for specific performance requirements. You must specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. **Tip** Specify an OU to restrict searches to certain user groups. For example, a subset of your users have instant messaging capabilities only. Include those users in an OU and then specify that as a search base.

Attribute Mappings

It is not possible to change the default attribute mappings in a service profile. If you plan to change any default attribute mappings, you must define the required mappings in a client configuration file.

Summary of Directory Integration Configuration Parameters

The following tables are a summary of all directory integration parameters.

Attribute Mapping

These parameters are used for attribute mapping with LDAP directory servers.

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

Directory Server Connection

These parameters are used for connecting to LDAP directory servers.

BDI Parameters	EDI Parameters
• BDILDAPServerType • BDIPresenceDomain • BDIPrimaryServerName • BDIServerPort1 • BDIUseJabberCredentials • BDIConnectionUsername • BDIConnectionPassword • BDIEnableTLS	• DirectoryServerType • ConnectionType • PrimaryServerName • SecondaryServerName • ServerPort1 • ServerPort2 • UseWindowsCredentials • ConnectionUsername • ConnectionPassword • UseSSL • UseSecureConnection

Contact Resolution and Directory Query

These parameters are used for contact resolution and directory queries with LDAP directory servers.

BDI Parameters	EDI Parameters
• BDIBaseFilter • BDIGroupBaseFilter • BDIUseANR • BDIPredictiveSearchFilter • BDISearchBase1 • BDIPhotoUriSubstitutionEnabled • BDIPhotoUriSubstitutionToken • BDIPhotoUriWithToken • BDIUseSIPURIToResolveContacts • BDIUriPrefix • BDIDirectoryUri • BDIDirectoryUriPrefix	• BaseFilter • GroupBaseFilter • PredictiveSearchFilter • DisableSecondaryNumberLookups • PhoneNumberMasks • SearchTimeout • UseWildcards • MinimumCharacterQuery • SearchBase1, SearchBase2, SearchBase3, SearchBase4, and SearchBase5 • PhotoUriSubstitutionEnabled • PhotoUriSubstitutionToken • PhotoUriWithToken • UseSIPURIToResolveContacts • UriPrefix • DirectoryUri • DirectoryUriPrefix

UDS

These parameters are used for interacting with UDS as a contact source.

- DirectoryServerType
- PresenceDomain
- UdsServer
- UdsPhotoUriWithToken

Directory Server Type Parameter

You specify the directory server type with the following parameter in the `jabber-config.xml` file:

Parameter	Value	Description
DirectoryServerType	BDI EDI UDS	Specifies the type of directory server to use. • BDI — Connect to a LDAP server. • EDI — Connect to a LDAP server. • UDS — Connect to UDS.

Directory Integration Parameters

The following sections lists details about the parameters you can configure for LDAP-based directory integration.

Attribute Mapping Parameters

The following table describes the parameters for mapping LDAP directory attributes.

BDI Parameter	EDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDICommonName	CommonName	cn	Yes	Yes	No
BDIDisplayName	DisplayName	displayName	Yes	Yes	Yes
BDIFirstname	Firstname	givenName	Yes	Yes	Yes
BDILastname	Lastname	sn	Yes	Yes	Yes
BDIEmailAddress	EmailAddress	mail	Yes	Yes	Yes
BDISipUri **Note** The client uses this parameter for intradomain federation, not URI dialing.	SipUri **Note** The client uses this parameter for intradomain federation, not URI dialing.	msRTCSIP-PrimaryUserAddress	Yes	Yes	Yes
BDIPhotoSource	PhotoSource	thumbnailPhoto	No	No	No
BDIBusinessPhone	BusinessPhone	telephoneNumber	Yes	No	No

BDI Parameter	EDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
BDIMobilePhone	MobilePhone	mobile	Yes	No	No
BDIHomePhone	HomePhone	homePhone	Yes	No	No
BDIOtherPhone	OtherPhone	otherTelephone	Yes	No	No
BDIDirectoryUri **Note** The client uses this parameter for URI dialing.	DirectoryUri **Note** The client uses this parameter for URI dialing.	mail	Yes	No	No
BDITitle	Title	title	Yes	No	No
BDICompanyName	CompanyName	company	Yes	Yes	No
BDIUserAccountName	UserAccountName	sAMAccountName	Yes	Yes	Yes
BDIDomainName	DomainName	EDI - userPrincipalName BDI - dn	Yes	Yes	No
BDICountry		co	Yes	No	No
BDILocation	Location	EDI - co BDI - location	Yes	No	No
BDINickname	Nickname	displayName	Yes	Yes	Yes
BDIPostalCode	PostalCode	postalCode	Yes	No	No
BDICity	City	l	Yes	Yes	No
BDIState	State	st	Yes	Yes	No
BDIStreetAddress	StreetAddress	streetAddress	Yes	No	No

Attributes on the Directory Server

You must index attributes on your LDAP directory server so that the client can resolve contacts.

If you use the default attribute mappings, ensure the following attributes are indexed:

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber

  Additionally, ensure you index the following attributes for secondary number queries:

  - otherTelephone
  - mobile
  - homePhone

Note By default secondary number queries are enabled in Cisco Jabber for Windows. You can disable secondary number queries with the DisableSecondaryNumberLookups parameter.

- msRTCSIP-PrimaryUserAddress

  Index msRTCSIP-PrimaryUserAddress for intradomain federation only.

Because Cisco Jabber for Windows connects to a Global Catalog server by default, you must ensure that all attributes reside on your Global Catalog server. You can replicate attributes to a Global Catalog server using an appropriate tool such as the Microsoft Active Directory Schema snap-in

- Replicating attributes to your Global Catalog server generates traffic between Active Directory servers in the domain. For this reason, replicate attributes to your Global Catalog server at a time when network traffic can handle extra load.
- If you do not want to replicate attributes to a Global Catalog server, configure Cisco Jabber to connect to a Domain Controller. However, the client queries single domains only when it connects to a Domain Controller.

Directory Connection Parameters

The following table describes parameters for configuring your LDAP directory connection:

BDI Parameter	EDI Parameter	Value	Description
	ConnectionType	0 1	Specifies if the client connects to a Global Catalog or a Domain Controller. • 0 (default) — Connect to a Global Catalog. • 1 — Connect to a Domain Controller. **Note** Default ports are as follows: • Global Catalog: 3268 • Domain Controller: 389
BDILDAPServerType		AD OpenLDAP	Specifies the type of LDAP directory server to which the client connects. • AD (default) — Connect to Active Directory. • OpenLDAP — Connect to OpenLDAP.
BDIPresenceDomain		Domain of the presence node.	Required parameter. Specifies the domain of the presence node. The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the user ID *amckenzie*. You specify *example.com* as the presence node domain. When the user logs in, the client constructs the IM address *amckenzie@example.com* for Adam McKenzie.

BDI Parameter	EDI Parameter	Value	Description
BDIPrimaryServerName	PrimaryServerName	IP address FQDN	Required parameter. Specifies the address of the primary directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server. **Note** Each time the client starts, it attempts to connect to the primary server. The client attempts to connect to the secondary server if: • The primary server is not available. • The primary server fails after the client connects to it. If the connection to the secondary server is successful, the client keeps the connection to the secondary server until the next restart. If the secondary server fails while the client is connected to it, the client attempts to connect to the primary server.
	SecondaryServerName	IP address FQDN	Specifies the address of the backup directory server. This parameter is required for manual connections where the client cannot automatically discover the directory server.
BDIServerPort1	ServerPort1	Port number	Specifies the port for the primary directory server.

BDI Parameter	EDI Parameter	Value	Description
ServerPort2	ServerPort2	Port number	Specifies the port for the backup directory server.
	UseWindowsCredentials	0 1	Specifies if the client uses Microsoft Windows usernames and passwords. • 0 — Do not use Windows credentials. Specify credentials with the ConnectionUsername and ConnectionPassword parameters. • 1 (default) — Use Windows credentials.
BDIUseJabberCredentials		true false	Specifies whether the client can use the presence server credentials to sign in to the directory server. • true — The client searches for the username and password in this order: 1 Client configuration file (BDIConnectionUsername and BDIConnectionPassword) 2 Presence server If the credentials are not present, the client tries to sign in anonymously. • false (default) — The client tries to sign in using the values of BDIConnectionUsername and BDIConnectionPassword in the client configuration file. If the parameters are not present, the client tries to sign in anonymously.

BDI Parameter	EDI Parameter	Value	Description
BDIConnectionUsername	ConnectionUsername	Username	Lets you manually specify a shared username that the client can use to authenticate with the directory server. **Important** The client transmits and stores this username as plain text. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a username in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials. Use only a well-known or public set of credentials for an account with read-only permissions to the directory.

BDI Parameter	EDI Parameter	Value	Description
BDIConnectionPassword	ConnectionPassword	Password	Lets you manually specify a shared password that the client can use to authenticate with the directory server. **Important** The client transmits and stores this password as plain text. By default, Cisco Jabber for Windows uses Integrated Windows Authentication when connecting to the directory server. This parameter lets you manually specify a password in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials. Use a well-known or public set of credentials for an account with read-only permissions to the directory.
BDIEnableTLS		true false	Use TLS to secure directory connections. • true — Use TLS. • false (default) — Do not use TLS.

BDI Parameter	EDI Parameter	Value	Description
	UseSSL	0 1	Use SSL for secure connections to the directory. • 0 (default) — Do not use SSL. • 1 — Use SSL. The SSL connection certificate must be present: • In the Microsoft Windows certificate store. • On the directory server to which the client connects. To establish an SSL connection, the server presents the client with the certificate. The client then validates the certificate from the server against the certificate in the store on the client computer. Default protocols and ports for SSL connections are as follows: • Global Catalog • Protocol: TCP • Port number: 3269 • Domain Controller • Protocol: TCP • Port number: 636

BDI Parameter	EDI Parameter	Value	Description
	UseSecureConnection	0 1	Specifies the mechanism for authentication with the directory server. • 0 — Use simple authentication. Set this value to connect to the directory server using simple binds. With simple authentication, the client transmits credentials in plain text. You can enable SSL to encrypt credentials with the UseSSL parameter. • 1 (default) — Use Generic Security Service API (GSS-API). GSS-API leverages the system authentication mechanism. In a Microsoft Windows environment, GSS-API lets you connect to the directory server using Kerberos-based Windows authentication.

Directory Query Parameters

The following table describes parameters for configuring how the client queries your LDAP directory:

BDI Parameter	EDI Parameter	Value	Description
BDIBaseFilter	BaseFilter	Base filter	Specifies a base filter for Active Directory queries. Specify a directory subkey name only to retrieve objects other than user objects when you query the directory. The default value for all clients is `(&(objectCategory=person)(objectClass=user)`. Configuration files can contain only valid XML character entity references. Use `&` instead of `&` if you specify a custom base filter.
BDIUseANR		true false	Specifies if Cisco Jabber issues a query using Ambiguous Name Resolution (ANR) when it performs a predictive search. • true (default) — Use ANR for predictive search. If you use OpenLDAP, the default value is false. • false — Do not use ANR for predictive search. Set the value to false if you integrate with a directory source other than Active Directory. **Important** Configure your directory server to set attributes for ANR if you want the client to search for those attributes.

BDI Parameter	EDI Parameter	Value	Description
BDIPredictiveSearchFilter	PredictiveSearchFilter	Search filter	Defines filters to apply to predictive search queries. You can define multiple, comma-separated values to filter search queries. **Note** This key is only used by Cisco Jabber for iPhone and iPad when BDIUseANR is set to false. And if BDI PredictiveSearchFilter is not set, the default search filter is used. The default EDI value is anr When Cisco Jabber for Windows performs a predictive search, it issues a query using ANR. This query disambiguates the search string and returns results that match the attributes that are set for ANR on your directory server. **Important** Configure your directory server to set attributes for ANR if you want the client to search for those attributes.
	DisableSecondaryNumberLookups	0 1	Specifies whether users can search for alternative contact numbers if the work number is not available, such as the mobile, home, or other number. • 0 (default) — Users can search for alternative contact numbers. • 1 — Users cannot search for alternative contact numbers.
	SearchTimeout	Number of seconds	Specifies the timeout period for queries in seconds. The default value is 5.

BDI Parameter	EDI Parameter	Value	Description
	UseWildcards	0 1	Enables wildcard searches. • 0 (default) — Do not use wildcards. • 1 — Use wildcards. If you use wildcards, it might take longer to search the directory.
	MinimumCharacterQuery	Numerical value	Sets the minimum number of characters in a contact name to query the directory. For example, if you set 2 as the value of this parameter, the client searches the directory when users enter at least two characters in the search field. The default value is 3.

BDI Parameter	EDI Parameter	Value	Description
BDISearchBase1	SearchBase1 SearchBase2 SearchBase3 SearchBase4 SearchBase5	Searchable organizational unit (OU) in the directory tree	Specifies a location in the directory server from which searches begin. In other words, a search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior. Active Directory does not typically require a search base. Specify search bases for Active Directory only for specific performance requirements. Specify a search base for directory servers other than Active Directory to create bindings to specific locations in the directory. **Tip** Specify an OU to restrict searches to certain user groups. For example, a subset of your users have IM capabilities only. Include those users in an OU and then specify that as a search base.

Base Filter Examples

The following are example base filters you can use to look up specific locations or objects.

Find only specific groups:

```
(&amp;(objectClass=user)(memberOf=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find a nested group within a group:

```
(&amp;(objectClass=user)(memberOf:search-oid:=cn=group-name,ou=Groups,dc=example,dc=com))
```

Find only enabled accounts and non-administrator accounts:

```
(&amp;(objectCategory=person)(objectClass=user)(!(userAccountControl:search-oid:=2))
(!(sAMAccountName=*_dbo))(!(sAMAccountName=*-admin)))
```

Phone Number Masks Parameter

Phone number masks parameter only applies to EDI. The following table describes the parameter to configure masks for phone number resolution:

Parameter	Value	Description
PhoneNumberMasks	Mask string	Specifies masks to use when users search for phone numbers. For example, a user receives a call from +14085550100. In the directory, this number is +(1) 408 555 0100. The following mask resolves the number: `+1408|+(#) ### ### ####` The length of mask strings cannot exceed the size restriction for registry subkey names.

Phone masks apply to phone numbers before the client searches your directory. If you configure phone masks correctly, directory searches succeed as exact query matches and prevent any impact to performance of your directory server.

The following table describes the elements you can include in a phone mask:

Element	Description
Phone number pattern	Provides a number pattern to retrieve phone numbers from your directory. To add a phone mask, you specify a number pattern that applies to the mask. For example, to specify a mask for searches that begin with +1408, you can use the following mask: +1408|+(#) ### ### #### To enable a mask to process phone numbers that have the same number of digits, but different patterns, use multiple masks with the same number of digits. For example, your company has site A and site B. Each site maintains a separate directory in which the phone numbers have different formats, such as the following: +(1) 408 555 0100 +1-510-5550101 The following mask ensures you can use both numbers correctly: +1408|+(#) ### ### ####|+1510|+#-###-#######.
Pipe symbol (|)	Separates number patterns and masks. For example, +1408|+(#) ### ### ####|+34|+(##) ### ####.

Element	Description
Wildcard character	Substitutes one or more characters for a subset of possible matching characters. Any wildcard character can exist in a phone mask. For example, an asterisk (*) represents one or more characters and can apply to a mask as follows: +3498|+##*##*###*####. Using this mask with the wildcard, a phone number search can match any of the following formats: +34(98)555 0199 +34 98 555-0199 +34-(98)-555.0199
Reverse mask	Applies a number pattern from right to left. For example, a mask of +3498|R+34 (98) 559 #### applied to +34985590199 results in +34 (98) 559 0199. You can use both forward and reverse masks.

Contact Photo Parameters

The following table describes parameters for configuring how the client retrieves contact photos from an LDAP directory.

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	true false	Specifies if photo URI substitution is enabled. • true — Photo URI substitution is enabled. • false (default) — Specifies if photo URI substitution is disabled.

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	Directory attribute	Specifies a directory attribute to insert in the photo URI; for example, sAMAccountName. Only the following attributes are supported for use with the PhotoURISubstitutionToken parameter: • Common Name • Display Name • First Name • Last Name • Nickname • Email Address • Photo Source • Business Phone • Mobile Phone • Home Phone • Preferred Phone • Other Phone • Title • Company Name • User Account Name • Domain Name • Location • Post Code • State • City • Street

BDI Parameter	EDI Parameter	Value	Description
BDIPhotoUriWithToken	PhotoUriWithToken	URI	Specifies a photo URI with a directory attribute as a variable value. For example: http://staffphoto.example.com/sAMAccountName.jpg The parameter applies to LDAP directory integrations. To configure photo URI substitution, you set the directory attribute as the value of BDIPhotoUriSubstitutionToken. **Restriction** The client must be able to retrieve the photos from the web server without credentials.
BDIPhotoSource	PhotoSource	Directory attribute	The name of a directory attribute that stores a contact photo as a binary object or a URI to a contact photo.

Contact Photo Retrieval

Cisco Jabber retrieves and displays contact photos with the following methods.

Note When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

URI substitution

Cisco Jabber dynamically builds a URL to contact photos with a directory attribute and a URL template.

To use this method, set the following values in your configuration file:

1. Specify `true` as the value of the BDIPhotoUriSubstitutionEnabled or PhotoUriSubstitutionEnabled parameter.
2. Specify a directory attribute to use as a dynamic token as the value of the BDIPhotoUriSubstitutionToken or PhotoUriSubstitutionToken parameter. For example,
```
<BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>
<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>
```
3. Specify the URL and the dynamic token as the value of the BDIPhotoUriWithToken or PhotoUriWithToken parameter. Use a direct URL for photo retrieval. Do not use redirected URLs. For example,
```
<BDIPhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>
<PhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</PhotoUriWithToken>
```

With the example values in the preceding steps, the `sAMAccountName` attribute might resolve to msmith in your directory. Cisco Jabber then takes this value and replaces the token to build the following URL: `http://staffphoto.example.com/msmith.jpg`.

Binary objects

Cisco Jabber retrieves the binary data for the photo from your database.

If you are using binary objects from Active Directory do not set BDIPhotoUriWithToken or PhotoUriWithToken.

To use this method to retrieve contact photos, specify the attribute that contains the binary data as the value of the BDIPhotoSource or PhotoSource parameter in the configuration. For example,

```
<BDIPhotoSource>jpegPhoto</BDIPhotoSource>
<PhotoSource>thumbnailPhoto</PhotoSource>
```

PhotoURL attribute

Cisco Jabber retrieves a URL from a directory attribute.

To use this method to retrieve contact photos, specify the attribute that contains the photo URL as the value of the BDIPhotoSource or PhotoSource parameter in the configuration. For example,

```
<BDIPhotoSource>photoUri</BDIPhotoSource>
<PhotoSource>photoUri</PhotoSource>
```

UDS Parameters

The following table provides details about the parameters you can use in the configuration file to connect to UDS and perform contact resolution and directory queries.

Parameter	Value	Description
PresenceDomain	Domain of the presence node.	Required parameter. Specifies the domain of the presence server. The client appends this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the following user ID: `amckenzie`. You specify `example.com` as the presence server domain. When the user logs in, the client constructs the following IM address for Adam McKenzie: `amckenzie@example.com`.
UdsServer	IP address FQDN	Specifies the address of the Cisco Unified Communications Manager User Data Service (UDS) server. This parameter is required for manual connections where the client cannot automatically discover the UDS server.

Parameter	Value	Description
UdsPhotoUriWithToken	URI	Specifies a photo URI with a directory attribute as a variable value; for example, `http://www.photo/url/path/%%uid%%.jpg`. This parameter applies to UDS directory integrations. You must specify this parameter to download contact photos in either of the following cases: • If you configure the DirectoryServerType parameter to use UDS. With this configuration, the client uses UDS for contact resolution when it is inside or outside of the corporate firewall. • If you deploy Expressway for Mobile and Remote Access. With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall. **Restriction** The client must be able to retrieve the photos from the web server without credentials.

Contact Photo Retrieval with UDS

Cisco Unified Communications Manager User Data Service (UDS) dynamically builds a URL for contact photos with a directory attribute and a URL template.

To resolve contact photos with UDS, you specify the format of the contact photo URL as the value of the UdsPhotoUriWithToken parameter. You also include a *%%uid%%* token to replace the contact username in the URL, for example,
`<UdsPhotoUriWithToken>http://server_name/%%uid%%.jpg</UdsPhotoUriWithToken>`

UDS substitutes the *%%uid%%* token with the value of the `userName` attribute in UDS. For example, a user named Mary Smith exists in your directory. The value of the `userName` attribute for Mary Smith is msmith. To resolve the contact photo for Mary Smith, Cisco Jabber takes the value of the `userName` attribute and replaces the *%%uid%%* token to build the following URL: `http://staffphoto.example.com/msmith.jpg`

Note When you change a photo in the Active Directory, the photo can take up to 24 hours to refresh in Cisco Jabber.

Important

- If you deploy Expressway for Mobile and Remote Access, the client automatically uses UDS for contact resolution when users connect to services from outside the corporate network. When you set up UDS contact resolution for Expressway for Mobile and Remote Access, you must add the web server on which you host the contact photos to the HTTP server allow list in your Cisco Expressway-C server configuration. The HTTP server allow list enables the client to access web services inside the corporate network.
- All contact photos must follow the format of the URL you specify as the value of UdsPhotoUriWithToken.

Contact Photo Formats and Dimensions

To achieve the best result with Cisco Jabber, your contact photos should have specific formats and dimensions. Review supported formats and optimal dimensions. Learn about adjustments the client makes to contact photos.

Contact Photo Formats

Cisco Jabber supports the following formats for contact photos in your directory:

- JPG
- PNG
- BMP

Important Cisco Jabber does not apply any modifications to enhance rendering for contact photos in GIF format. As a result, contact photos in GIF format might render incorrectly or with less than optimal quality. To obtain the best quality, use PNG format for your contact photos.

Contact Photo Dimensions

Tip The optimum dimensions for contact photos are 128 pixels by 128 pixels with an aspect ratio of 1:1.

128 pixels by 128 pixels are the maximum dimensions for local contact photos in Microsoft Outlook.

The following table lists the different dimensions for contact photos in Cisco Jabber.

Location	Dimensions
Audio call window	128 pixels by 128 pixels

Location	Dimensions
Invitations and reminders, for example: • Incoming call windows • Meeting reminder windows	64 pixels by 64 pixels
Lists of contacts, for example: • Contact lists • Participant rosters • Call history • Voicemail messages	32 pixels by 32 pixels

Contact Photo Adjustments

Cisco Jabber adjusts contact photos as follows:

- Resizing—If contact photos in your directory are smaller or larger than 128 pixels by 128 pixels, the client automatically resizes the photos. For example, contact photos in your directory are 64 pixels by 64 pixels. When Cisco Jabber retrieves the contact photos from your directory, it resizes the photos to 128 pixels by 128 pixels.

  Tip Resizing contact photos can result in less than optimal resolution. For this reason, use contact photos that are 128 pixels by 128 pixels so that the client does not automatically resize them.

- Cropping—Cisco Jabber automatically crops nonsquare contact photos to a square aspect ratio, or an aspect ratio of 1:1 where the width is the same as the height.
- Portrait orientation—If contact photos in your directory have portrait orientation, the client crops 30 percent from the top and 70 percent from the bottom.

  For example, if contact photos in your directory have a width of 100 pixels and a height of 200 pixels, Cisco Jabber needs to crop 100 pixels from the height to achieve an aspect ratio of 1:1. In this case, the client crops 30 pixels from the top of the photos and 70 pixels from the bottom of the photos.
- Landscape orientation—If contact photos in your directory have landscape orientation, the client crops 50 percent from each side.

  For example, if contact photos in your directory have a width of 200 pixels and a height of 100 pixels, Cisco Jabber needs to crop 100 pixels from the width to achieve an aspect ratio of 1:1. In this case, the client crops 50 pixels from the right side of the photos and 50 pixels from the left side of the photos.

Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

Domain Controller Connection

To connect to a Domain Controller, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1

The following is an example configuration:

```
<Directory><DirectoryServerType>EDI</DirectoryServerType>
<ConnectionType>1</ConnectionType></Directory>
```

Manual Server Connections for Cisco Jabber for Windows

To manually connect to a directory server, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	FQDN IP address
ServerPort1	Port number
SecondaryServerName	FQDN IP address
ServerPort2	Port number

The following is an example configuration:

```
<Directory>
<DirectoryServerType>EDI</DirectoryServerType>
<PrimaryServerName>primary-server-name.domain.com</PrimaryServerName>
<ServerPort1>1234</ServerPort1>
<SecondaryServerName>secondary-server-name.domain.com</SecondaryServerName>
<ServerPort2>5678</ServerPort2>
</Directory>
```

UDS Integration

To integrate with UDS, set the following parameters.

Parameter	Value
DirectoryServerType	UDS
UdsServer	IP address of the UDS server
UdsPhotoUriWithToken	Contact photo URL
PresenceDomain **Note** This parameter is only applicable to Phone Mode.	Server address of your presence domain

Note Configure the DirectoryServerType parameter to UDS only if you want to use UDS for all contact resolution (that is, from inside and outside the corporate firewall).

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>UDS</DirectoryServerType>
  <UdsServer>11.22.33.444</UdsServer>
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

LDAP Integration with Expressway for Mobile and Remote Access

When you deploy Expressway for Mobile and Remote Access with an LDAP directory integration, the client uses:

- LDAP when inside the corporate firewall
- UDS when outside the corporate firewall

Note LDAP is the default configuration, so it is not necessary to include the DirectoryServerType parameter in your client configuration file.

To ensure that the client can resolve contact photos from both inside and outside your corporate firewall, set the following parameters.

Parameter	Value
BDIPhotoUriWithToken	Contact photo URL when inside the corporate firewall
UdsPhotoUriWithToken	Contact photo URL when outside the corporate firewall

The following is an example configuration:

```
<Directory>
  <BDIPhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>
```

```
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

Simple Authentication for Cisco Jabber for Windows

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>0</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Does not use SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result of the simple bind, the client transmits the credentials in the payload of the bind request in plain text.

Simple Authentication for Mobile Clients and Cisco Jabber for Mac

Simple authentication lets you connect to a directory server using simple binds, as in the following example configuration:

```
<BDIEnableTLS>False</BDIEnableTLS>
<BDIConnectionUsername>username</BDIConnectionUsername>
<BDIConnectionPassword>password</BDIConnectionPassword>
<BDIServerPort1>389/3268</BDIServerPort1>
```

This configuration specifies that the client:

- Does not use SSL.
- Uses simple authentication.
- Uses custom credentials.
- Uses port 389/3268 for non-TLS.

As a result of the simple bind, the client transmits the credentials in the payload of the bind request in plain text.

Simple Authentication with SSL for Cisco Jabber for Windows

Enable SSL in directory server connections with the UseSSL parameter. You can use SSL to encrypt credentials when you use simple authentication, as in the following example configuration:

```
<UseWindowsCredentials>0</UseWindowsCredentials>
<UseSSL>1</UseSSL>
<UseSecureConnection>0</UseSecureConnection>
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword>password</ConnectionPassword>
```

This configuration specifies that the client:

- Does not use Microsoft Windows credentials.
- Uses SSL.
- Uses simple authentication.
- Uses custom credentials.

As a result, the client uses SSL to encrypt the credentials in the client configuration.

Simple Authentication with SSL for Mobile Clients

Enable SSL in directory server connections with the BDIEnableTLS parameter. You can use SSL to encrypt credentials when you use simple authentication, as in the following example configuration:

```
<BDIEnableTLS>True</BDIEnableTLS>
<BDIConnectionUsername>username</BDIConnectionUsername>
<BDIConnectionPassword>password</BDIConnectionPassword>
<BDIServerPort1>636/3269</BDIServerPort1>
```

This configuration specifies that the client:

- Uses SSL.
- Uses simple authentication.
- Uses custom credentials.
- Uses port 636/3269 for TLS.

As a result, the client uses SSL to encrypt the credentials in the client configuration.

OpenLDAP Integration

You can integrate with OpenLDAP using anonymous binds or authenticated binds.

Anonymous Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1
PrimaryServerName	IP address Hostname
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)

Parameter	Value
UserAccountName	Unique identifier such as UID or CN
BaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	UID or other search filter

The following is an example configuration:

```
<Directory>
 <DirectoryServerType>EDI</DirectoryServerType>
 <ConnectionType>1</ConnectionType>
 <PrimaryServerName>11.22.33.456</PrimaryServerName>
 <UseWindowsCredentials>0</UseWindowsCredentials>
 <UseSecureConnection>1</UseSecureConnection>
 <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
 <UserAccountName>uid</UserAccountName>
  <BaseFilter>(&amp;(objectClass=inetOrgPerson)</BaseFilter>
 <PredictiveSearchFilter>uid</PredictiveSearchFilter>
</Directory>
```

Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	BDI
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	True
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as uid or cn
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter

The following is an example configuration:

```
<Directory>
 <DirectoryServerType>BDI</DirectoryServerType>
```

```
 <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
 <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
 <BDIEnableTLS>True</BDIEnableTLS>
 <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
 <BDIServerPort1>636/3269</BDIServerPort1>
 <BDIUserAccountName>uid</BDIUserAccountName>
 <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
 <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
</Directory>
```

Authenticated Binds for Cisco Jabber for Windows

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
ConnectionType	1
PrimaryServerName	IP address Hostname
UserWindowsCredentials	0
UseSecureConnection	0
SearchBase1	Root of the directory service or the organizational unit (OU)
UserAccountName	Unique identifier such as UID or CN
BaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	UID or other search filter
ConnectionUsername	Username
ConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <ConnectionType>1</ConnectionType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <UserWindowsCredentials>0</UserWindowsCredentials>
  <UseSecureConnection>0</UseSecureConnection>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
  <UserAccountName>uid</UserAccountName>
  <BaseFilter>(&amp;(objectClass=inetOrgPerson)</BaseFilter>
  <PredictiveSearchFilter>uid</PredictiveSearchFilter>
  <ConnectionUsername>cn=lds-read-only-user,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
</Directory>
```

Authenticated Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with OpenLDAP using authenticated binds, set the following parameters:

Parameter	Value
DirectoryServerType	BDI
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	False
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIServerPort1	The port for the primary directory server
BDIUserAccountName	Unique identifier such as UID or CN
BDIBaseFilter	Object class that your directory service uses; for example, inetOrgPerson.
BDIPredictiveSearchFilter	(Optional) UID or other search filter
BDIConnectionUsername	Username
BDIConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>BDI</DirectoryServerType>
  <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>False</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIServerPort1>389/3268</BDIServerPort1>
  <BDIUserAccountName>uid</BDIUserAccountName>
  <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>
  <BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
</Directory>
```

AD LDS Integration

You can integrate with AD LDS or ADAM using specific configurations.

Anonymous Binds for Cisco Jabber for Windows

To integrate with AD LDS or ADAM using anonymous binds, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <SearchBase1>dc=adam,dc=test</SearchBase1>
</Directory>
```

Anonymous Binds for Mobile Clients and Cisco Jabber for Mac

To integrate with AD LDS or ADAM using anonymous binds, set the following parameters:

Parameter	Value
BDIPrimaryServerName	IP address Hostname
BDIServerPort1	Port number
BDISearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIServerPort1>50000</BDIServerPort1>
  <BDISearchBase1>dc=adam,dc=test</BDISearchBase1>
</Directory>
```

Windows Principal User Authentication

To integrate with AD LDS or ADAM using authentication with the Microsoft Windows principal user, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServerName	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	1
ConnectionUsername	Username
ConnectionPassword	Password
UserAccountName	Unique identifier such as UID or CN
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <DirectoryServerType>EDI</DirectoryServerType>
  <PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>1</UseSecureConnection>
  <ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
  <UserAccountName>cn</UserAccountName>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

AD LDS Principal User Authentication for Cisco Jabber for Windows

To integrate with AD LDS or ADAM using authentication with the AD LDS principal user, set the following parameters:

Parameter	Value
DirectoryServerType	EDI
PrimaryServer	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	0

Parameter	Value
ConnectionUsername	Username
ConnectionPassword	Password
UserAccountName	Unique identifier such as UID or CN
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
<DirectoryServerType>EDI</DirectoryServerType>
<PrimaryServerName>11.22.33.456</PrimaryServerName>
  <ServerPort1>50000</ServerPort1>
  <UseWindowsCredentials>0</UseWindowsCredentials>
  <UseSecureConnection>0</UseSecureConnection>
  <ConnectionUsername>cn=administrator,dc=cisco,dc=com</ConnectionUsername>
  <ConnectionPassword>password</ConnectionPassword>
  <UserAccountName>cn</UserAccountName>
  <SearchBase1>ou=people,dc=cisco,dc=com</SearchBase1>
</Directory>
```

AD LDS Principal User Authentication for Mobile Clients and Cisco Jabber for Mac

To integrate with AD LDS or ADAM using authentication with the AD LDS principal user, set the following parameters:

Parameter	Value
BDIPrimaryServerName	IP address Hostname
BDIServerPort1	Port number
BDIConnectionUsername	Username
BDIConnectionPassword	Password
BDIUserAccountName	Unique identifier such as uid or cn
BDISearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIServerPort1>50000</BDIServerPort1>
  <BDIConnectionUsername>cn=administrator,dc=cisco,dc=com</BDIConnectionUsername>
  <BDIConnectionPassword>password</BDIConnectionPassword>
  <BDIUserAccountName>cn</BDIUserAccountName>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
</Directory>
```