Directory Integration

DirectoryServerType

Applies to all clients.

Specifies the type of directory server you want to use.

The values used for this parameter are:

- BDI — Connect to a LDAP server. Used for Cisco Jabber for MAC and mobile clients.
- EDI — Connect to a LDAP server. Used for Cisco Jabber for Windows clients.
- UDS — Connect to UDS (Cisco Unified Communications Manager server). Used for all Cisco Jabber clients. Applicable for Expressway Mobile and Remote Access.

Example: `<DirectoryServerType>BDI</DirectoryServerType>`

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
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

BDI Parameter	EDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
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 for the clients. This lets clients resolve contacts.

To use the default attribute mappings, you must index the following attributes:

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

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

  - otherTelephone

- mobile
- homePhone

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

- msRTCSIP-PrimaryUserAddress

Since Cisco Jabber for Windows connects to a Global Catalog server by default, you must ensure that all attributes reside on your Global Catalog server. You can replicate attributes to a Global Catalog server using an appropriate tool such as the Microsoft Active Directory Schema Snap-in. You can choose either to replicate or not to replicate attributes to your Global Catalog server:

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

EDI Parameters

The EDI parameters apply to Cisco Jabber for Windows.

Directory Connection

ConnectionType

Specifies whether 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

Example: `<ConnectionType>1</ConnectionType>`

PrimaryServerName

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

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

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

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

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

SecondaryServerName

Specifies the address of the backup directory server.

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

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

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

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

ServerPort1

Specifies the port for the primary directory server.

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

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

ServerPort2

Specifies the port for the backup directory server.

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

Example:`<ServerPort2>345</ServerPort2>`

UseWindowsCredentials

Specifies whether 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.

Example: `<UseWindowsCredentials>0</UseWindowsCredentials>`

ConnectionUsername

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

By default, Cisco Jabber for Windows uses Integrated Windows Authentication to connect with the directory server. You can use this parameter in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.

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

Important The client transmits and stores this username as plain text.

Example: `<ConnectionUsername>username</ConnectionUsername>`

ConnectionPassword

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

By default, Cisco Jabber for Windows uses Integrated Windows Authentication to connect with the directory server. You can use this parameter in scenarios where it is not possible to authenticate with the directory server with the user's Microsoft Windows credentials.

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

Important The client transmits and stores this password as encrypted unless you have configured your LDAP settings for plaintext transmission.

The value for this parameter is the shared password.

Example: `<ConnectionPassword>password</ConnectionPassword>`

UseSSL

Specifies if SSL is used for secure connections to the directory.

- 0— Do not use SSL.
- 1 (default) — Use SSL.

Example: `<UseSSL>1</UseSSL>`

To establish an SSL connection, the server sends an SSL connection certificate to the client. The client then validates the certificate from the server against the certificate in the store on the client computer. You must ensure that the SSL connection certificate is present:

- In the Microsoft Windows certificate store.
- On the directory server to which the client connects.

Default protocols and ports for SSL connections are as follows:

	Global Catalog	Domain Controller
Protocol	TCP	TCP
Port number	3269	636

UseSecureConnection

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).

  Set this value to use system authentication mechanism with GSS-API. In a Microsoft Windows environment, GSS-API lets you connect to the directory server using Kerberos-based Windows authentication.

Example: `<UseSecureConnection>0</UseSecureConnection>`

Directory Query

BaseFilter

Specifies a base filter for Active Directory queries.

You must specify a directory subkey name if you want to retrieve objects other than user objects when you query the directory.

Configuration files can contain only valid XML character entity references. To specify a custom base filter, you must use `&` instead of `&`.

The default value for all clients is `(&(objectCategory=person)( objectClass=user)`.

Example: `<BaseFilter>(&(objectCategory=person) (memberOf=cn=group-name))</BaseFilter>`

GroupBaseFilter

Specifies a base filter for Active Directory Enterprise Group queries.

The default value for all clients is:

`(&(objectCategory=group)(!(groupType:1.2.840.113556.1.4.803:=2147483648))` (ensure you remove any spaces inserted in this value prior to using it).

Example:

```
<GroupBaseFilter>(&amp;(objectCategory=person)(memberOf=cn=group-name))</GroupBaseFilter>
```

PredictiveSearchFilter

Defines the attribute set for predictive search LDAP queries. You can define multiple, comma-separated values to filter search queries.

This setting is only read when "UseANR" is set to False, or when connecting to a non-Active Directory server. If UseANR is not set to any value, Jabber will use a default attribute set for predictive search queries.

Default values are created based on attribute mappings for the following Jabber parameters:

- mail
- username
- displayname
- givenname
- surname
- nickname
- sipURI

Typical mappings for these attributes are as follows:

Jabber Parameter	Active Directory attribute	OpenLDAP
mail	mail	mail
username	SAMAccountName	uid
displayname	displayName	cn
givenname	givenName	givenName
nickname	displayName	

Jabber Parameter	Active Directory attribute	OpenLDAP
sipURI	msRTCSIP-PrimaryUserAddress	mail
surname	sn	sn

If your directory server doesn't support ANR format queries, you can populate this setting if you want to customize the attribute set queried for predictive search queries.

DisableSecondaryNumberLookups

Specifies whether users can search for alternative contact numbers if the work number is not available, such as the mobile, home, or other number.

- 0 (default) — Users can search for alternative contact numbers.
- 1 — Users cannot search for alternative contact numbers.

Example: `<DisableSecondaryNumberLookups>1</DisableSecondaryNumberLookups>`

SearchTimeout

Specifies the timeout period for queries in seconds.

The value for this parameter is number of seconds. The default value is 5.

Example: `<SearchTimeout>6</SearchTimeout>`

UseWildcards

Specifies whether users can use wildcard searches.

- 0 (default) — Do not use wildcards.
- 1 — Use wildcards.

Note If you use wildcards, it might take longer to search the directory.

Example: `<UseWildcards>1</UseWildcards>`

MinimumCharacterQuery

Sets the minimum number of characters in a contact name that a user needs to enter to query the name from the directory.

The only value for this parameter is a numerical value. The default value is 3.

For example, if you set 2 as the value of this parameter, the client searches the directory when users enter at least two characters in the search field.

Example: `<MinimumCharacterQuery>2</MinimumCharacterQuery>`

SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5

Specifies a location in the directory server from which searches begin.

A search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree.

Active Directory doesn't typically require a search base. Specify search bases for Active Directory only when you have specific performance requirements. When specifying search bases, you must also specify search base for directory servers other than Active Directory to create bindings to specific locations in the directory.

The value for this parameter is a searchable Organizational Unit (OU) in the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior.

Tip You can specify an OU to restrict searches to certain user groups. For example, a subset of your users has IM capabilities only. Include those users in an OU and then specify that as a search base.

Example:`<SearchBase1>OU=Users1</SearchBase1>`

GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5

Specifies a location in the directory server from which Enterprise Group searches begin.

A search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree.

You can specify the value of up to five search bases in your Organizational Unit (OU) to override the default behavior.

The value for this parameter is a searchable OU in the directory tree.

Example: `<GroupSearchBase1>OU=Group1</GroupSearchBase1>`

IM Address Scheme

UseSipUriToResolveContacts

Specifies the IM address scheme that the Cisco IM and Presence service uses.

- true — Use the Directory URI scheme.
- false (default) — Use the User ID @[Default Domain] scheme.

Example: `<UseSipUriToResolveContacts>true</UseSipUriToResolveContacts>`

UriPrefix

Specifies a prefix to remove from the SipUri parameter.

The value is a prefix string.

For example, sip: may prefix the msRTCSIP-PrimaryUserAddress directory attribute.

Example: `<UriPrefix>sip:</UriPrefix>`

SipUri

Specifies the directory attribute field that the IM Address scheme field is mapped to.

The value for this parameter can be one of the following directory attribute fields:

- mail
- msRTCSIP-PrimaryUserAddress

Example: `<SipUri>msRTCSIP-PrimaryUserAddress</SipUri>`

Contact Photo

PhotoUriSubstitutionEnabled

Specifies if a URI is used to display photos.

- true — Photo URI substitution is enabled.
- false (default) — Photo URI substitution is disabled.

Example: `<PhotoUriSubstitutionEnablede>true</PhotoUriSubstitutionEnabled>`

PhotoUriSubstitutionToken

Specifies the token in the Photo URI that is used to create the path to the photos.

Only the following attributes are supported for use with the PhotoURISubstitutionToken parameter:

- Common Name
- Display Name
- First Name
- Last Name
- Nickname
- Email Address
- Photo Source
- Business Phone

- Mobile Phone
- Home Phone
- Preferred Phone
- Other Phone
- Title
- Company Name
- User Account Name
- Domain Name
- Location
- Post Code
- State
- City
- Street

Important When using this parameter, you must ensure the PhotoUriSubstitutionEnabled parameter is set to true.

The value for this parameter is a directory attribute.

Example: `<PhotoUriSubstitutionToken>sAMAccountName</PhotoUriSubstitutionToken>`

PhotoUriWithToken

Specifies a photo URI with a directory attribute as a variable value.

The parameter applies to LDAP directory integrations.

Restriction The client must be able to retrieve the photos from the web server without credentials.

To configure photo URI substitution, you set the directory attribute as the value of PhotoUriSubstitutionToken.

The value for this parameter is a URI.

Example:

```
<PhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</PhotoUriWithToken>
```

PhotoSource

The name of a directory attribute that stores a contact photo as a binary object or a URI to a contact photo.

The value is a directory attribute.

Example: `<PhotoSource>thumbnailPhoto</PhotoSource>`

Tip If you are using attributes such as “jpegPhoto” and “thumbnailPhoto”, ensure that these are added to the Global Catalog on the Active Directory.

PhoneNumberMasks

Specifies masks to use when users search for phone numbers.

For example, a user receives a call from +14085550100. In the directory, this number is +(1) 408 555 0100. The following mask resolves the number: `+1408|+(#) ### ### ####`. The length of mask strings cannot exceed the size restriction for registry subkey names.

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

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

Element	Description
Phone number pattern	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|+(##) ### ####.
Wildcard character	Substitutes one or more characters with 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

Element	Description
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.

The only value for this parameter is mask string.

Example: `<PhoneNumberMasks>+1408|+(#) ### ### ####</PhoneNumberMasks>`

BDI Parameters

The BDI parameters apply to Cisco Jabber for Mac and mobile clients.

Directory Connection

BDILDAPServerType

Specifies the type of LDAP directory server to which the client connects.

- AD (default) — Connect to Active Directory.
- OpenLDAP — Connect to OpenLDAP.

Example: `<BDILDAPServerType>OpenLDAP</BDILDAPServerType>`

BDIPresenceDomain

Specifies the domain of the presence node. This is a required parameter.

The only value for this parameter is domain of the presence node.

The client adds this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the user ID *amckenzie*. You specify *example.com* as the presence node domain.

When the user logs in, the client constructs the IM address *amckenzie@example.com* for Adam McKenzie.

Example: `<BDIPresenceDomain>example.com</BDIPresenceDomain>`

BDIPrimaryServerName

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

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

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

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

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

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

BDIServerPort1

Specifies the port for the primary directory server.

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

Example:`<BDIServerPort1>636</BDIServerPort1>`

BDIUseJabberCredentials

Specifies whether the client can use the Cisco IM and Presence service credentials to sign in to the directory server.

- true — The client searches for the username and password to sign in to the directory server in this order:
  1. Values of BDIConnectionUsername and BDIConnectionPassword in the client configuration file
  2. Credentials in Cisco IM and Presence service

  If the credentials are not present, the client tries to sign in anonymously.
- false (default) — The client tries to sign in to the directory server 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.

Example: `<BDIUseJabberCredentials>true</BDIUseJabberCredentials>`

BDIConnectionUsername

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

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

Important The client transmits and stores this username as plain text.

The only value for this parameter is username.

Example: `<BDIConnectionUsername>admin@example.com</BDIConnectionUsername>`

BDIConnectionPassword

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 encrypted unless you have configured your LDAP settings for plaintext transmission.

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

The value for this parameter is the shared password.

Example: `<BDIConnectionPassword>connectionpwd</BDIConnectionPassword>`

BDIEnableTLS

Specifies whether to use TLS for secure directory connections.

- true — Use TLS.
- false (default) — Do not use TLS.

Example: `<BDIEnableTLS>true</BDIEnableTLS>`

Directory Query

BDIBaseFilter

Specifies a base filter for Active Directory queries.

You must specify a directory subkey name if you want to retrieve objects other than user objects when you query the directory.

Configuration files can contain only valid XML character entity references. To specify a custom base filter, you must use `&amp;` instead of `&`.

The default value for all clients is `(&(objectCategory=person)( objectClass=user)`.

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

- Find only specific groups:
  Example: `(&(objectClass=user)(memberOf=cn=group-name,ou=Groups,dc=example,dc=com))`
- Find a nested group within a group:
  Example:
  `(&(objectClass=user)(memberOf:search-oid:=cn=group-name,ou=Groups,dc=example,dc=com))`
- Find only enabled accounts and non-administrator accounts:
  Example:
  `<(&(objectCategory=person)(objectClass=user)(!(userAccountControl:search-oid:=2))`
  `(!(sAMAccountName=*_dbo))(!(sAMAccountName=*-admin)))>`

Example: `<BDIBaseFilter>(&(objectCategory=person)(memberOf=cn=group-name))</BDIBaseFilter>`

BDIGroupBaseFilter

Specifies a base filter for Active Directory Enterprise Group queries.

The default value for all clients is:

`(&(objectCategory=group)(!(groupType:1.2.840.113556.1.4.803:=2147483648))` (ensure you remove any spaces inserted in this value prior to using it).

Example:`<BDIGroupBaseFilter>(&(objectClass=user)(memberOf=cn=group-name))</BDIGroupBaseFilter>`

BDIUseANR

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.

Example: `<BDIUseANR>false</BDIUseANR>`

BDIPredictiveSearchFilter

Defines filters to apply to predictive search queries.

You can define multiple, comma-separated values to filter search queries.

The default value is anr.

Important Configure your directory server to set attributes for ANR, if you want the client to search for those attributes.

The value for this parameter is a search filter.

Note

- If the BDIUseANR parameter is set to false, this key is only used by Cisco Jabber for iPhone and iPad.
- If the BDIPredictiveSearchFilter parameter is not set, the default search filter is used.

Example: `<BDIPredictiveSearchFilter>uid</BDIPredictiveSearchFilter>`

BDISearchBase1

Specifies a location in the directory server from which searches begin.

A search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree.

Active Directory doesn't typically require a search base. Specify search bases for Active Directory only when you have specific performance requirements. When specifying search bases, you must also specify search base for directory servers other than Active Directory to create bindings to specific locations in the directory.

The value for this parameter is a searchable Organizational Unit (OU) in the directory tree. You can specify the value of up to five search bases in your OU to override the default behavior.

Tip You can specify an OU to restrict searches to certain user groups. For example, a subset of your users has IM capabilities only. Include those users in an OU and then specify that as a search base.

Example: `<BDISearchBase1>CN=Users,DC=cisco,DC=com</BDISearchBase1>`

BDIGroupSearchBase1

Specifies a location in the directory server from which Enterprise Group searches begin.

A search base is the root from which the client executes a search. By default, the client searches from the root of the directory tree.

You can specify the value of up to five search bases in your Organizational Unit (OU) to override the default behavior.

The value for this parameter is a searchable OU in the directory tree.

Example: `<BDIGroupSearchBase1>ou=people,dc=cisco,dc=com</BDIGroupSearchBase1>`

IM Address Scheme

BDIUseSipUriToResolveContacts

Specifies the IM address scheme that the Cisco IM and Presence service uses.

- true — Use the Directory URI scheme.
- false (default) — Use the User ID @[Default Domain] scheme.

Example: `<BDIUseSipUriToResolveContacts>true</BDIUseSipUriToResolveContacts>`

BDIUriPrefix

Specifies a prefix to remove from the SipUri parameter.

The value is a prefix string.

For example, sip: may prefix the msRTCSIP-PrimaryUserAddress directory attribute.

Example: `<BDIUriPrefix>sip:</BDIUriPrefix>`

BDISipUri

Specifies the directory attribute field that the IM Address scheme field is mapped to.

The value for this parameter can be one of the following directory attribute fields:

- mail
- msRTCSIP-PrimaryUserAddress

```
<BDISipUri>msRTCSIP-PrimaryUserAddress</BDISipUri>
```

Contact Photo

BDIPhotoUriSubstitutionEnabled

Specifies if a URI is used to display photos.

- true — Photo URI substitution is enabled.
- false (default) — Photo URI substitution is disabled.

Example: `<BDIPhotoUriSubstitutionEnabled>true</BDIPhotoUriSubstitutionEnabled>`

BDIPhotoUriSubstitutionToken

Specifies the token in the Photo URI that is used to create the path to the photos.

Only the following attributes are supported for use with the BDIPhotoURISubstitutionToken parameter:

- Common Name
- Display Name
- First Name
- Last Name
- Nickname
- Email Address
- Photo Source
- Business Phone
- Mobile Phone
- Home Phone
- Preferred Phone
- Other Phone
- Title
- Company Name
- User Account Name
- Domain Name
- Location
- Post Code
- State
- City
- Street

Important When using this parameter, you must ensure the BDIPhotoUriSubstitutionEnabled parameter is set to true.

The value for this parameter is a directory attribute.

Example: `<BDIPhotoUriSubstitutionToken>sAMAccountName</BDIPhotoUriSubstitutionToken>`

BDIPhotoUriWithToken

Specifies a photo URI with a directory attribute as a variable value.

The parameter applies to LDAP directory integrations.

Restriction The client must be able to retrieve the photos from the web server without credentials.

To configure photo URI substitution, you set the directory attribute as the value of BDIPhotoUriSubstitutionToken.

The value for this parameter is a URI.

Example:
```
<BDIPhotoUriWithToken>http://staffphoto.example.com/sAMAccountName.jpg</BDIPhotoUriWithToken>
```

BDIPhotoSource

The name of a directory attribute that stores a contact photo as a binary object or a URI to a contact photo.

The value is a directory attribute.

For Cisco Jabber for Mac, the default values are:

- AD: thumbnaiPhoto
- OpenLDAP: jpegPhoto

To use a photo with AD, remove any BDIPhotoSource attributes in jabber-config.xml. You need not specify thumbnailPhoto as the attribute, because the client uses thumbnailPhoto as the default. Simply upload the user image to the thumbnailPhoto attribute in AD.

Example: `<BDIPhotoSource>thumbnailPhoto</BDIPhotoSource>`

Tip If you are using attributes such as “jpegPhoto” and “thumbnailPhoto”, ensure that these are added to the Global Catalog on the Active Directory.

UDS Parameters

Use the UDS parameters to connect to the UDS server and to perform contact resolution and directory queries.

The UDS parameters apply to all the Cisco Jabber clients.

Directory Connection

PresenceDomain

Specifies the domain of the presence node. This is a required parameter.

The only value for this parameter is domain of the presence node.

The client adds this domain to the user ID to create an IM address. For example, a user named Adam McKenzie has the user ID *amckenzie*. You specify *example.com* as the presence node domain.

When the user logs in, the client constructs the IM address *amckenzie@example.com* for Adam McKenzie.

Example: `<PresenceDomain>example.com</PresenceDomain>`

UdsServer

Specifies the address of the Cisco Unified Communications Manager User Data Service (UDS) server.

This parameter is required for manual connections where the client cannot automatically discover the UDS server.

- IP address — Use IP address for UDS server.
- FQDN — Use FQDN for UDS server.

Example: `<UdsServer>ccm1</UdsServer>`

IM Address Scheme

UdsPhotoUriWithToken

Specifies a photo URI with a directory attribute as a variable value.

This parameter applies to UDS directory integrations. You must specify this parameter to download contact photos in either of the following cases:

- If you configure the DirectoryServerType parameter to use UDS. With this configuration, the client uses UDS for contact resolution when it is inside or outside the corporate firewall.
- If you deploy Expressway for Mobile and Remote Access. With this deployment, the client automatically uses UDS for contact resolution when it is outside the corporate firewall.

Restriction The client must be able to retrieve the photos from the web server without credentials.

The value for this parameter is a URI.

Example: `<UdsPhotoUriWithToken>http://www.photo/url/path/%%uid%%.jpg</UdsPhotoUriWithToken>`

UseSIPURIToResolveContacts

Specifies the IM address scheme that the IM and Presence Service uses.

- true — Use the Directory URI scheme.
- false (default) — Use the User ID @[Default Domain] scheme.

Example: `<UseSIPURIToResolveContacts>true</UseSIPURIToResolveContacts>`

UriPrefix

Specifies a prefix to remove from the SipUri or BDISipUri parameter.

The only value is a prefix string.

For example, sip: may prefix the msRTCSIP-PrimaryUserAddress directory attribute.

Example: `<UriPrefix>sip:</UriPrefix>`

SipUri

Specifies the directory attribute field to which the IM Address scheme field is mapped.

The value for this parameter can be one of the following directory attribute fields:

- mail
- msRTCSIP-PrimaryUserAddress

Example: `<SipUri>msRTCSIP-PrimaryUserAddress</SipUri>`

Directory Server Configuration Examples

This section describes supported integration scenarios and provides example configurations.

Domain Controller Connection

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

Parameter	Value
ConnectionType	1

The following is an example configuration:

```
<Directory>
<ConnectionType>1</ConnectionType></Directory>
```

Manual Server Connections for Cisco Jabber for Windows

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

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

The following is an example configuration:

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

UDS Integration

To integrate with UDS, set the following parameters.

Parameter	Value
DirectoryServerType	UDS
UdsServer	IP address of the UDS server
UdsPhotoUriWithToken	Contact photo URL
PresenceDomain **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
PhotoUriWithToken	Contact photo URL when inside the corporate firewall
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>
  <PhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</PhotoUriWithToken>
  <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</BDIConnecitonPassword>
<ServerPort1>636</<ServerPort1>
<ServerPort1>3269</ServerPort1>
```

This configuration specifies that the client:

- Uses SSL.
- Uses simple authentication.
- Uses custom credentials.
- Uses port 636 or 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
ConnectionType	1
PrimaryServerName	IP address Hostname
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)
GroupSearchBase1	Root of the Enterprise Group 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.
GroupBaseFilter	Object class that your Enterprise Group directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	UID or other search filter

The following is an example configuration:

```
<Directory>

 <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
BDILDAPServerType	OpenLDAP

Parameter	Value
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	True
BDISearchBase1	Root of the directory service or the organizational unit (OU)
BDIGroupSearchBase1	Root of the Enterprise Group 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.
BDIGroupBaseFilter	Object class that your Enterprise Group directory service uses; for example, inetOrgPerson.
(Optional) BDIPredictiveSearchFilter	uid or other search filter

The following is an example configuration:

```
<Directory>

 <BDILDAPServerType>OpenLDAP</BDILDAPServerType>
 <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
 <BDIEnableTLS>True</BDIEnableTLS>
 <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
 <BDIServerPort1>636</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
ConnectionType	1
PrimaryServerName	IP address Hostname
UserWindowsCredentials	0
UseSecureConnection	0

Parameter	Value
SearchBase1	Root of the directory service or the organizational unit (OU)
GroupSearchBase1	Root of the Enterprise Group 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.
GroupBaseFilter	Object class that your Enterprise Group directory service uses; for example, inetOrgPerson.
PredictiveSearchFilter	UID or other search filter
ConnectionUsername	Username
ConnectionPassword	Password

The following is an example configuration:

```
<Directory>
  <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
BDILDAPServerType	OpenLDAP
BDIPrimaryServerName	IP address Hostname
BDIEnableTLS	False
BDISearchBase1	Root of the directory service or the organizational unit (OU)

Parameter	Value
BDIGroupSearchBase1	Root of the Enterprise Group 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.
BDIGroupBaseFilter	Object class that your Enterprise Group directory service uses; for example, inetOrgPerson.
BDIPredictiveSearchFilter	(Optional) UID or other search filter
BDIConnectionUsername	Username
BDIConnectionPassword	Password

The following is an example configuration:

```
<Directory>
<BDILDAPServerType>OpenLDAP</BDILDAPServerType>
  <BDIPrimaryServerName>11.22.33.456</BDIPrimaryServerName>
  <BDIEnableTLS>False</BDIEnableTLS>
  <BDISearchBase1>ou=people,dc=cisco,dc=com</BDISearchBase1>
  <BDIGroupSearchBase1>ou=people,dc=cisco,dc=com</BDIGroupSearchBase1>
  <BDIServerPort1>636</BDIServerPort1>
  <BDIUserAccountName>uid</BDIUserAccountName>
  <BDIBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIBaseFilter>
  <BDIGroupBaseFilter>(&amp;(objectClass=inetOrgPerson)</BDIGroupBaseFilter>
  <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
PrimaryServerName	IP address Hostname
ServerPort1	Port number

Parameter	Value
UseWindowsCredentials	0
UseSecureConnection	1
SearchBase1	Root of the directory service or the organizational unit (OU)

The following is an example configuration:

```
<Directory>
  <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
PrimaryServerName	IP address Hostname
ServerPort1	Port number

Parameter	Value
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>
  <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
PrimaryServer	IP address Hostname
ServerPort1	Port number
UseWindowsCredentials	0
UseSecureConnection	0
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>
<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>
```