Directory Integration

- Directory Parameters, on page 1
- CDI Parameters, on page 3
- Attribute Mapping Parameters, on page 15
- UDS Parameters, on page 18
- Directory Server Configuration Examples, on page 20

Directory Parameters

The following table lists the BDI and EDI parameters, indicating the CDI parameter name or if it doesn't apply to Jabber 11.8 or later.

BDI Parameters	EDI Parameters	CDI Parameters
-	DirectoryServerType	DirectoryServerType
-	ConnectionType	-
BDILDAPServerType	-	-
BDIPresenceDomain	PresenceDomain	PresenceDomain
BDIPrimaryServerName	PrimaryServerName	PrimaryServerName
-	SecondaryServerName	SecondaryServerName
BDIServerPort1	ServerPort1	ServerPort1
-	ServerPort2	ServerPort2
-	UseWindowCredentials	-
BDIUseJabberCredentials	-	-
BDIConnectionUsername	ConnectionUsername	ConnectionUsername
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL

BDI Parameters	EDI Parameters	CDI Parameters
-	UseSecureConnection	-
BDIUseANR	UseANR	UseANR
BDIBaseFilter	BaseFilter	BaseFilter
BDIGroupBaseFilter	GroupBaseFilter	GroupBaseFilter
BDIUseANR	-	-
BDIPredictiveSearchFilter	PredictiveSearchFilter	PredictiveSearchFilter
-	DisableSecondaryNumberLookups	DisableSecondaryNumberLookups
-	SearchTimeout	SearchTimeout
-	UseWildcards	UseWildcards
-	MinimumCharacterQuery	MinimumCharacterQuery
BDISearchBase1	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5	SearchBase1, SearchBase2, SearchBase3, SearchBase4, SearchBase5
BDIGroupSearchBase1	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5	GroupSearchBase1, GroupSearchBase2, GroupSearchBase3, GroupSearchBase4, GroupSearchBase5
BDIUseSipUriToResolveContacts	UseSipUriToResolveContacts	UseSipUriToResolveContacts
BDIUriPrefix	UriPrefix	UriPrefix
BDISipUri	SipUri	SipUri
BDIPhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	PhotoUriSubstitutionToken
BDIPhotoUriWithToken	PhotoUriWithToken	PhotoUriWithToken
BDIPhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName

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

CDI Parameters

The CDI parameters apply to all clients.

Directory Connection

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>`

ConnectionUsername

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

By default, Jabber desktop clients use Kerberos or client certificate authentication. Only use this parameter in deployments where you can't authenticate with the directory server using either Kerberos or client certificate authentication.

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, Jabber desktop clients use Kerberos or client certificate authentication. Only use this parameter in deployments where you can't authenticate with the directory server using either Kerberos or client certificate authentication.

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

Default setting: True

The connection to the LDAP server uses SSL by default using the LDAPS protocol.

Setting this to False uses the plaintext LDAP protocol. The plaintext LDAP protocol will also be chosen if the LDAP port is either 389 or 3268 and the UseSSL configuration key is not set.

Note The configuration key when set overrides any automatic determination of the protocol.

UseANR

Default setting (all clients): True

Enable/disable the use of Ambiguous Name Resolution (ANR) when performing predictive search queries.

When set to True, Jabber constructs LDAP queries using ANR for predictive search.

If set to False, Jabber constructs a complex query for use in predictive search.

ANR is disabled if Jabber is connecting to an OpenLDAP server. It is enabled only when connecting to an Active Directory server.

The format of the query used for non-ANR servers is set using the "PredictiveSearchFilter" parameter.

Example: <UseANR>false</UseANR>

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>(&(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	
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)—Don't 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>`

LdapSupportedMechanisms

Applies to all clients.

Specifies the order for authenticating with the LDAP server.

Each of the mechanisms specified below must be supported by the Contact Service and the LDAP server.

Use a space to separate multiple authentication mechanisms.

- **GSSAPI (default)** —Kerberos v5. Supported by desktop clients only.
- **EXTERNAL**—SASL external.
- **PLAIN**—Simple LDAP bind (anonymous bind is a subset of simple bind). Used by default if ConnectionUsername and ConnectionPassword parameters or LDAP_UseCredentialsFrom parameter are present

Example 1: `<LdapSupportedMechanisms>GSSAPI EXTERNAL PLAIN</ LdapSupportedMechanisms>`

In this example, Jabber checks first if GSSAPI is supported, then attempts to authenticate. If GSSAPI is not supported, then Jabber checks if EXTERNAL is supported, then attempts to authenticate. If neither are supported, then Jabber attempts PLAIN authentication.

Example 2: `<LdapSupportedMechanisms>PLAIN</LdapSupportedMechanisms>`

In this example, Jabber uses PLAIN authentication only.

EnableEmployeeNumber

Applies to Cisco Jabber for Windows.

Fetches the employee number from the LDAP server when a user searches for it using Jabber.

- 0 or false (default)—Employee number is disabled.
- 1 or true—Employee number is enabled.

Example: `<EnableEmployeeNumber>0</EnableEmployeeNumber>`

UseLdapReferral

Applies to Cisco Jabber for Windows and Cisco Jabber for Android.

Specifies if the client uses LDAP referrals when attempting to resolve contacts.

Values:

- 0 (Default)—Disables LDAP referrals
- 1—Enables LDAP referrals

Example: <UseLdapReferral>1</UseLdapReferral>

LDAP_UseCredentialsFrom

Applies to all Cisco Jabber clients for on-premises deployments.

Specifies which credentials are used by Cisco Jabber when connecting to the directory server.

- Voicemail—use voicemail credentials when connecting to the directory server.
- Exchange—use the credentials that Cisco Jabber uses to connect to Microsoft Exchange when connecting to the directory server.
- CUCM—use Cisco Unified Communications Manager credentials when connecting to the directory server.

Example: `<LDAP_UseCredentialsFrom>CUCM</LDAP_UseCredentialsFrom>`

When this parameter is set, users are not given the option to enter their directory credentials manually in the Options window. You can also set directory credentials using the Cisco Unified Communications Manager service profile or using the CDI directory integration parameters you defined in the `jabber-config.xml` file. It is not recommended to use both synchronized credentials and administrator-defined credentials.

Keep in mind that you may need to use the LdapUserDomain parameter to define the domain to authenticate against the LDAP server (where applicable). For example, the authentication ID would be <*CUCM Username*>@<LdapUserDomain>.

Note Do not use the LDAP_UseCredentialsFrom parameter with any of the following parameters because they can cause conflicting configuration:

- LdapAnonymousBinding
- ConnectionUsername and ConnectionPassword
- UseWindowsCredentials

LdapUserDomain

Applies to all Cisco Jabber clients for on-premises deployments.

Specifies the domain to be appended to the username when connecting to the LDAP server. This is useful when the LDAP server requires a UPN or email-based account to authenticate with. This parameter is used with the LDAP_UseCredentialsFrom parameter.

The username is appended with the @ symbol followed by the value specified by LdapUserDomain. This value is then used to connect to the LDAP server. For example, a user named Adam McKenzie has the user ID *amckenzie* and the LdapUserDomain is *example.com*, then the username that authenticates with the LDAP server is *amckenzie@example.com*.

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

LdapDNSForestDomain

Applies to all the Cisco Jabber clients.

Restriction Use this parameter only in jabber-config files for non-Windows environments.

Jabber uses a DNS SRV query to discover the Global Catalog by first reading the DNSFORESTNAME environment variable. If the environment variable is not present, Jabber next uses a Windows API to retrieve the DNS forest name. If you want Jabber to behave similarly on non-Windows environments, place the DNS forest name in LdapDNSForestDomain in the jabber-config file.

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: `<PhotoUriSubstitutionEnabled>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
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>`

ContactSearchSource

Applies to all clients.

Prerequisites: Jabber team messaging mode is enabled.

Specifies what sources should be used for Jabber searches for environments running Jabber team messaging mode. With the search results, you'll see the person's profile picture, and be able to call them.

This parameter is ignored if you configure the ContactProfileSearch parameter with CI as the value.

- CI (default)—Jabber users can search for contacts that are in the Common Identity (CI) in the Teams directory.

- CI-UDS-LDAP—Jabber users can search for contacts from the company directory (on UDS/LDAP), as well as the CI.

Note If you use this value, you might need to also use DirectoryServerType.

Example: `<ContactSearchSource>CI-UDS-LDAP</ContactSearchSource>`

ContactProfileSource

Applies to all clients.

Prerequisites: Jabber team messaging mode is enabled.

Define the source for the profiles of your users' contacts for environments running Jabber team messaging mode. With the search results, you'll see the person's profile picture, and be able to call them.

- CI —Profile information from the Common Identity (CI) in the Teams directory. If you set this value, then the ContactSearchSource parameter is ignored, and predictive search is only on CI.
- CI-UDS-LDAP (default)—Jabber will get the profile information from UDS or LDAP. The profile information from CI has higher priority over the one from UDS/LDAP if any user details have conflicts, such as their photo or display name.

Note If you use this value, you might need to also use DirectoryServerType.

Example: `<ContactProfileSource>CI-UDS-LDAP</ContactProfileSource>`

DirectoryServerType

Applies to all clients.

Specifies the type of directory server you want to use for contact resolution. Jabber consults this parameter when you set ContactSearchSource or ContactProfileSource to `CI-UDS-LDAP`.

If you use Expressway for MRA, Jabber ignores this parameter and uses UDS.

The values used for this parameter are:

- LDAP—Connect to an LDAP server.
- UDS—Connect to UDS (Cisco Unified Communications Manager server). This value is used for all Cisco Jabber clients and is applicable for Expressway Mobile and Remote Access.

Example: `<DirectoryServerType>LDAP</DirectoryServerType>`

Attribute Mapping Parameters

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

CDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
CommonName	cn	Yes	Yes	No
DisplayName	displayName	Yes	Yes	Yes
Firstname	givenName	Yes	Yes	Yes
Lastname	sn	Yes	Yes	Yes
EmailAddress	mail	Yes	Yes	Yes
SipUri **Note** The client uses this parameter for intradomain federation, not URI dialing.	msRTCSIP-PrimaryUserAddress	Yes	Yes	Yes
PhotoSource	thumbnailPhoto	No	No	No
BusinessPhone	telephoneNumber	Yes	No	No
MobilePhone	mobile	Yes	No	No
HomePhone	homePhone	Yes	No	No
OtherPhone	otherTelephone	Yes	No	No
DirectoryUri **Note** The client uses this parameter for URI dialing.	mail	Yes	No	No
Title	title	Yes	No	No
CompanyName	company	Yes	Yes	No
UserAccountName	sAMAccountName	Yes	Yes	Yes
DomainName	userPrincipalName	Yes	Yes	No
	co	Yes	No	No
Location		Yes	No	No
Nickname	displayName	Yes	Yes	Yes
PostalCode	postalCode	Yes	No	No

CDI Parameter	Directory Attribute	Exists in Global Catalog by Default	Is Indexed by Default	Set for Ambiguous Name Resolution (ANR) by Default
City	l	Yes	Yes	No
State	st	Yes	Yes	No
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.

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 parameter.

The only value is a prefix string.

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

If SipUri is not set to msRTCSIP-PrimaryUserAddress, delete the tag -<UriPrefix>sip:</UriPrefix>

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>`

EmailAddress

Applies to all the Cisco Jabber clients.

Specifies which attribute in User Data Service (UDS) is the email address. Configure this parameter with the value mail.

Example:

```
<EmailAddress>mail</EmailAddress>
```

Note This parameter supports both LDAP and UDS queries in the latest Jabber versions.

DirectoryUriPrefix

Applies to all Cisco Jabber clients.

Specifies a prefix to remove from the DirectoryUri value only if the data comes from LDAP.

For example, if your directory URI is `sip:amckenzie@example.com`, set the following:

```
<DirectoryUriPrefix>sip:</DirectoryUriPrefix>
```

MaxWordsOfFirstName

Applies to all the Cisco Jabber clients.

This parameter applies to UDS directory integrations and specifies the maximum number of words that a user's first name can have in the predictive search. The default value for a user's first name is 2 words and there is no limit for the maximum words.

Example: <MaxWordsOfFirstName>2</MaxWordsOfFirstName>

MaxWordsOfLastName

Applies to all the Cisco Jabber clients.

This parameter applies to UDS directory integrations and specifies the maximum number of words that a user's last name can have in the predictive search. The default value for a user's last name is 2 words and there is no limit for the maximum words.

Example: <MaxWordsOfLastName>2</MaxWordsOfLastName>

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>
```

KerberosConfiguration

Applies to Cisco Jabber for desktop

You can add the KerberosConfiguration parameter in the jabber-config.xml file. The parameter value is written to the disk as the MIT-Kerberos configuration file.

If you don't configure this parameter, Jabber can only connect to the Active Directory domain joined by the client machine to perform a directory search. To connect to other Active Directory domains to which the client machine doesn't belong, configure domain_realm mapping.

For example, in a Multi-Forest environment, suppose you have two forests deployed in your AD infrastructure. The user accounts are in forest 1 and the resource is in forest 2. In this case, configure `domain1.com` as the user domain and configure `domain2.com` and `child.domain2.com` as the resource domain. You establish a trust relationship between forest 1 and forest 2.

If users sign in from `domain1.com` and want to access the resource domain, configure KerberosConfiguration with the appropriate values in jabber-config.xml.

Note If the Kerberos configuration doesn't work when typed in a single line, try typing it in multiple lines as in this example.

Example:

```
<Directory>
  <KerberosConfiguration>
    [domain_realm]
      .domain1.com = DOMAIN1.COM
      .child.domain1.com = CHILD.DOMAIN1.COM
  </KerberosConfiguration>
</Directory>
```

Manual Server Connections for Cisco Jabber

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.

Parameter	Value
UdsPhotoUriWithToken	contact photo URL when outside the corporate firewall.

The following is an example configuration:

```
<Directory>
  <PhotoUriWithToken>http://photo.example.com/sAMAccountName.jpg</PhotoUriWithToken>
  <UdsPhotoUriWithToken>http://server-name/%%uid%%.jpg</UdsPhotoUriWithToken>
</Directory>
```

Simple Authentication for Cisco Jabber

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

```
<ConnectionUsername>username</ConnectionUsername>
<ConnectionPassword> password</ConnectionPassword>
```