Contact Source

- What is a Contact Source?, on page 1
- Why Do I Need a Contact Source?, on page 2
- When to Configure Contact Source Servers, on page 2
- Contact Source Options for Cisco Directory Integration , on page 3
- LDAP Prerequisites, on page 10
- Jabber ID Attribute Mapping, on page 11
- Local Contact Sources, on page 12
- Custom Contact Sources, on page 12
- Contact Caching, on page 12
- Resolving Duplicate Contacts, on page 12
- Dial Plan Mapping, on page 13
- Cisco Unified Communication Manager UDS for Mobile and Remote Access, on page 13
- Cloud Contact Source, on page 14
- Contact Photo Formats and Dimensions, on page 14

What is a Contact Source?

A contact source is a collection of data for users. When users search for contacts or add contacts in the Cisco Jabber client, the contact information is read from a contact source.

Cisco Jabber retrieves the information from the contact source to populate contact lists, update contact cards in the client and other areas that display contact information. When the client receives any incoming communications, for example an instant message or a voice/video call, the contact source is used to resolve the contact information.

Contact Source Servers

Note All Jabber clients support the LDAPv3 standard for directory integration. Any directory server that supports this standard is compatible with these clients.

You can use the following contact source servers with Cisco Jabber:

- Active Directory Domain Services for Windows Server 2012 R2

- Active Directory Domain Services for Windows Server 2008 R2
- Cisco Unified Communications Manager User Data Server (UDS). Cisco Jabber supports UDS using Cisco Unified Communications Manager version 10.5 or higher.
- OpenLDAP
- Active Directory Lightweight Directory Service (AD LDS) or Active Directory Application Mode (ADAM)

Why Do I Need a Contact Source?

Cisco Jabber uses the contact source in the following ways:

- Users search for a contact—The client takes the information entered and searches in the contact source. Information is retrieved from the contact source and the client will display the available methods to interact with the contact.
- Client receives incoming notification—The client will take the information from the incoming notification and resolve the URI, number, JabberID with a contact from the contact source. The client will display the contact details in the alert.

When to Configure Contact Source Servers

Note Install Cisco Jabber on a workstation that is registered to an Active Directory domain. In this environment, you do not need to configure Cisco Jabber 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 service if you plan to use one of the following services as the contact source:

- Active Directory Service
- 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.

Contact Source Options for Cisco Directory Integration

In on-premises deployments, the client requires one of the following contact sources to resolve directory look ups for user information:

- Lightweight Directory Access Protocol (LDAP)—If you have a corporate directory, you can use the following LDAP-based contact source options to configure your directory as the contact source:
  - Cisco Directory Integration (CDI)—Use this contact source option to deploy all clients.
- Cisco Unified Communications Manager User Data Service (UDS)—If you do not have a corporate directory or if your deployment includes users connecting with Expressway Mobile and Remote Access, you can use this option.

Lightweight Directory Access Protocol

How Cisco Directory Integration Works with LDAP

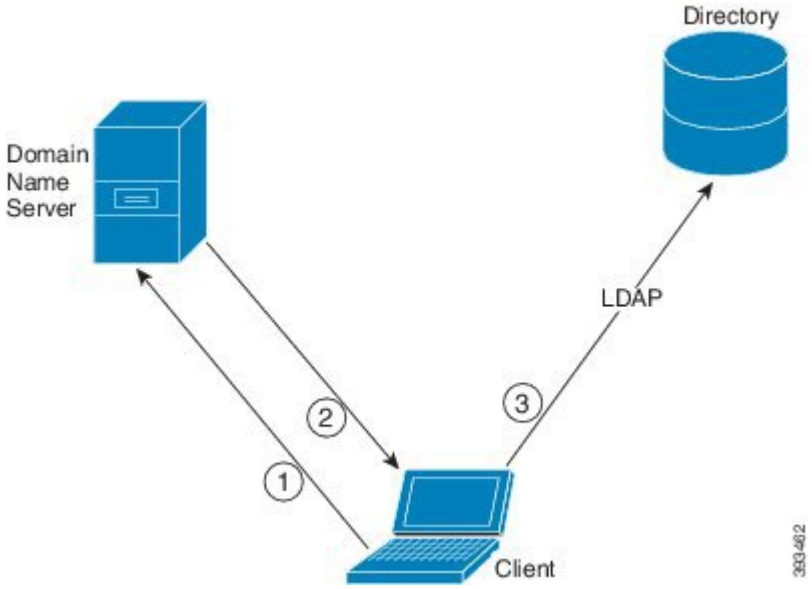
CDI uses service discovery to determine the LDAP server.

The following are the default settings for on-premises deployments with CDI:

- Cisco Jabber integrates with Active Directory as the contact source.
- Cisco Jabber automatically discovers and connects to a Global Catalog.

Automatic Service Discovery—Recommended

We recommend that you use service discovery to automatically connect and authenticate with the Global Catalog (GC) server or the LDAP server. If you want to customize your deployment, review the options for providing the LDAP server information and the authentication options that are available. Jabber first sends DNS queries to the GC domain to discover the GC servers. If it doesn't discover the GC servers, Jabber then send DNS queries to the LDAP domain to discover the LDAP servers.



When there is a GC available, the client does the following:

1. Gets the DNS domain from the workstation and looks up the SRV record for the GC.
2. Retrieves the address of the GC from the SRV record.
3. Connects to the GC with the signed-in user's credentials.

Discovery Using the Global Catalog Domain

Jabber attempts to discover GC servers with a DNS SRV query. First, Jabber gets the GC domain:

1. If available, Jabber uses the DNSFORESTNAME environment variable as the GC domain.
2. If DNSFORESTNAME is not available, Jabber checks the following for the GC domain:
   - On Windows, Jabber calls the Windows `DsGetDcName` API to get `DnsForestName`.
   - On non-Windows platforms, Jabber reads LdapDNSForestDomain from `jabber-config.xml`.

After Jabber gets the GC domain, it sends a DNS SRV query to get the GC server address:

- On Windows, Jabber checks if `SiteName` is available through Windows `DsGetSiteName` API:
  - If `SiteName` exists, Jabber sends out the DNS SRV query, `_gc._tcp.SiteName._sites.GCDomain`, to get the GC server address.
  - If `SiteName` doesn't exist or no SRV record is returned for `_gc._tcp.SiteName._sites.GCDomain`, Jabber sends out the DNS SRV query, `_gc._tcp.GCDomain`, to get the GC server address.
- On a non-Windows platform, Jabber sends out the DNS SRV query, `_gc._tcp.GCDomain`, to get the GC server address.

Discovery Using the LDAP Domain

If Jabber cannot discover a GC server, it then attempts to discover the LDAP domain:

1. If available, Jabber uses the USERDNSDOMAIN environment variable as the LDAP domain.
2. If USERDNSDOMAIN is not available, Jabber reads LdapUserDomain from `jabber-config.xml`.
3. If LdapUserDomain is not available, Jabber uses the email domain with which the user signed in as the LDAP domain.

After Jabber gets the LDAP Domain, it sends a DNS SRV query to get the LDAP server address:

- On Windows, Jabber checks if `SiteName` is available through Windows `DsGetSiteName` API.
  - If `SiteName` exists, Jabber sends out the DNS SRV query, `_ldap._tcp.SiteName.sites.LdapDomain`, to get the LDAP server address.
  - If `SiteName` doesn't exist or no SRV record is returned for `_ldap._tcp.SiteName.sites.LdapDomain`, Jabber sends out the DNS SRV query, `_ldap._tcp.LdapDomain`, to get the LDAP server address.
- On a non-Windows platform, Jabber sends out the DNS SRV query, `_ldap._tcp.LdapDomain`, to get the LDAP server address.

Once Jabber connects to the LDAP server, it reads the LDAP server's `SupportedSaslMechanisms` attribute that specifies a list and order of authentication mechanisms to use.

Manual Configuration for the LDAP Service

Manual Configuration for the LDAP Service

1. You can configure the PrimaryServerName parameter to define a specific LDAP server for Jabber to connect to.
2. You can configure the LdapSupportedMechanisms parameter in the `jabber-config.xml` file to override the list from the supportedSaslMechanisms attribute.

   The Contact Service and the LDAP server must support each of these mechanisms. Use a space to separate multiple values.

   - GSSAPI – Kerberos v5
   - EXTERNAL – SASL external
   - PLAIN (default) – Simple LDAP bind, anonymous is a subset of simple bind.

   Example:

   ```
   <LdapSupportedMechanisms>GSSAPI EXTERNAL PLAIN</LdapSupportedMechanisms>
   ```

3. If necessary, configure the LdapUserDomain parameter to set the domain that Jabber uses to authenticate with the LDAP server. For example:

   ```
   CUCMUsername@LdapUserDomain
   ```

LDAP Considerations

Cisco Directory Integration (CDI) parameters replace the Basic Directory Integration (BDI) and Enhanced Directory Integration (EDI) parameters. CDI parameters apply to all clients.

Cisco Jabber Deployment Scenarios

Scenario 1: If you are new to Jabber in 11.8

We recommend that you use service discovery to automatically connect and authenticate with the LDAP server. If you want to customize your deployment, review the options for providing the LDAP server information and the authentication options that are available.

Scenario 2: If you are upgrading to 11.8 from an EDI configuration

If your configuration only uses EDI parameters, then Jabber will read the EDI parameters and use those for your directory source integration. We still recommend that you upgrade your EDI parameters and replace them with the equivalent CDI parameters.

Scenario 3: If you are upgrading to 11.8 from a BDI configuration

If your configuration only uses BDI parameters, you must update the BDI parameters to the equivalent CDI parameters. For example, for the BDIPrimaryServerName you need to replace the parameter with PrimaryServerName. The BDIEnableTLS is replaced with the UseSSL parameter.

Scenario 4: If you are upgrading to 11.8 from a mixed EDI/BDI configuration

If your configuration uses both EDI and BDI, you must review your configuration for BDI as Jabber will use the EDI parameters when connecting to the LDAP server.

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

BDI Parameters	EDI Parameters	CDI Parameters
BDIConnectionPassword	ConnectionPassword	ConnectionPassword
BDIEnableTLS	UseSSL	UseSSL
-	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
BDIPhotoUriSubstitutionEnab led	PhotoUriSubstitutionEnabled	PhotoUriSubstitutionEnabled
BDIPhotoUriSubstitutionToken	PhotoUriSubstitutionToken	PhotoUriSubstitutionToken
BDIPhotoUriWithToken	PhotoUriWithToken	PhotoUriWithToken
BDIPhotoSource	PhotoSource	PhotoSource
LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom	LDAP_UseCredentialsFrom
LDAPUserDomain	LDAPUserDomain	LDAPUserDomain
-	-	LdapSupportedMechanisms

BDI Parameters	EDI Parameters	CDI Parameters
BDICommonName	CommonName	CommonName
BDIDisplayName	DisplayName	DisplayName
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

Cisco Unified Communications Manager User Data Service

User Data Service (UDS) is a REST interface on Cisco Unified Communications Manager that provides contact resolution.

UDS is used for contact resolution in the following cases:

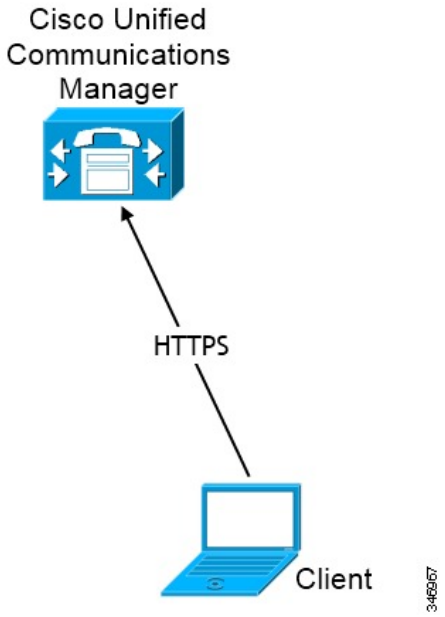
- If you set the DirectoryServerType parameter to use a value of UDS in the client configuration file.

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 Remote and Mobile Access.

  With this configuration, the client automatically uses UDS for contact resolution when it is outside of the corporate firewall.

You synchronize contact data into Cisco Unified Communications Manager from a directory server. Cisco Jabber then automatically retrieves that contact data from UDS.



Contact Resolution with Multiple Clusters

For contact resolution with multiple Cisco Unified Communications Manager clusters, synchronize all users on the corporate directory to each cluster. Provision a subset of those users on the appropriate cluster.

For example, your organization has 40,000 users. 20,000 users reside in North America. 20,000 users reside in Europe. Your organization has the following Cisco Unified Communications Manager clusters for each location:

- `cucm-cluster-na` for North America
- `cucm-cluster-eu` for Europe

In this example, synchronize all 40,000 users to both clusters. Provision the 20,000 users in North America on `cucm-cluster-na` and the 20,000 users in Europe on `cucm-cluster-eu`.

When users in Europe call users in North America, Cisco Jabber retrieves the contact details for the user in Europe from `cucm-cluster-na`.

When users in North America call users in Europe, Cisco Jabber retrieves the contact details for the user in North America from `cucm-cluster-eu`.

Extended UDS Contact Source

Extend the contact search from UDS to your LDAP server. In Cisco Unified Communications Manager 11.5(1) or later, you can configure if Jabber searches your LDAP server.

LDAP Prerequisites

Cisco Jabber searches the contact source using various attributes, not all of these attributes are indexed by default. To ensure efficient searches the attributes used by Cisco Jabber must be indexed.

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

- sAMAccountName
- displayName
- sn
- name
- proxyAddresses
- mail
- department
- givenName
- telephoneNumber
- otherTelephone
- mobile
- homePhone
- msRTCSIP-PrimaryUserAddress

LDAP Service Account

In Unified Communications Manager Release 12.5(1) SU2, Unified CM added support for securely passing encrypted LDAP credentials in the Service Profile. This update secures access to your directory by ensuring that the password is always stored and sent in an encrypted format. This change includes encryption during these processes:

- Directory access authentication
- Client configuration file downloads
- BAT imports/exports
- Upgrades

For more details, see the *Release Notes for Cisco Unified Communications Manager and the IM and Presence Service, Release 12.5(1) SU2*.

In Jabber 12.8 with this Unified CM release or later, we take advantage of this capability by downloading the LDAP credentials as part of User Profile after end-user authentication.

To connect Jabber to an LDAP server, define how LDAP authenticates Jabber users:

- The default option is that Jabber automatically connects to the contact source server using Kerberos or client certificates (SASL External). We recommend this option as it's the most secure.
- If you define credentials in a service profile or in the `jabber-config.xml` file, they always take precedence over the default option.
- If you configure the LdapSupportedMechanisms parameter with the PLAIN value, but don't configure the directory profile username or password, then users can enter their directory credentials into the clients directly.
- Otherwise, if you connect to a secure port in the service profile, then you can define how Jabber connects to the contact source server. You define it by specifying the Cisco Unified Communications Manager credentials in the LDAP_UseCredentialsFrom parameter in the `jabber-config.xml` file.
- If the previous options aren't available, then use a well-known set of credentials provided by the Service Profile or the `jabber-config.xml` file. This option is the least secure. Jabber uses an account to authenticate with the contact source server. We recommend that this account has read-only access to the directory and is a commonly known public set of credentials. In this case, all Jabber users use these credentials for searches.

Note From Cisco Unified Communications Manager 12.0 version onwards, you can't configure username and password in the service profile. Jabber users get an option to authenticate themselves for using directory services. Users get a notification when they sign in to Jabber for the first time. If they don't authenticate themselves that first time, then they get an alert when they are trying to access contact list.

Jabber ID Attribute Mapping

The LDAP attribute for user ID is sAMAccountName. This is the default attribute.

If the attribute for the user ID is other than sAMAccountName, and you're using the default IM address scheme in Cisco Unified Communications Manager IM and Presence Service, you must specify the attribute as the value for the parameter in your client configuration file as follows:

The CDI parameter is UserAccountName. <UserAccountName>attribute-name</UserAccountName>

If you do not specify the attribute in your configuration, and the attribute is other than sAMAccountName, the client cannot resolve contacts in your directory. As a result, users do not get presence and cannot send or receive instant messages.

Search Jabber IDs

Cisco Jabber uses the Jabber ID to search for contact information in the directory. There are a few options to optimize searching in the directory:

- **Search base**—By default the client starts a search at the root of a directory tree. You can use search bases to specify a different search start or to restrict searches to specific 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.

- **Base Filter**—Specify a directory subkey name only to retrieve objects other than user objects when you query the directory.
- **Predictive Search Filter**—You can define multiple, comma-separated values to filter search queries. The default value is ANR(Ambiguous name resolution.)

For more information on these options, see the chapter on directory integration in the *Parameters Reference Guide for Cisco Jabber*.

Local Contact Sources

Cisco Jabber has the ability to access and search local contact sources. These local contact sources include the following:

- Local contacts stored in Microsoft Outlook are accessed by Cisco Jabber for Windows.
- Local contacts stored in IBM Notes are accessed by Cisco Jabber for Windows (from release 11.1).
- Local address book contacts are accessed by Cisco Jabber for Mac, Cisco Jabber for Android and Cisco Jabber for iPhone and iPad.

Custom Contact Sources

Cisco Jabber for all clients provides users with the ability to import custom contacts into their client.

Contact Caching

Cisco Jabber creates a local cache. Among other things, the cache stores the user's contact list. When a user searches for somebody in their contact list, Jabber searches the local cache for a match before starting a directory search.

If a user searches for somebody who is not in their contact list, Jabber first searches the local cache and then searches the company directory. If the user then starts a chat or a call with this contact, Jabber adds the contact to the local cache.

The local cache information expires after 24 hours.

Resolving Duplicate Contacts

Contacts in Jabber can come from different sources. Jabber can find matches for the same contact in several contact sources. In that case, Jabber determines which records match the same person and combines all data for that person. To determine if a record in one of the contact sources matches the contact, Jabber looks for these fields in the following order:

1. **Jabber ID (JID)**—If the records have a JID, Jabber matches the records on that basis. Jabber does not further compare based on the mail or phone number fields.
2. **Mail**—If the records have a mail field, Jabber matched the records on that basis. Jabber does not further compare the records based on phone numbers.
3. **Phone Number**—If the records have a phone number, Jabber matches the records on that basis.

As Jabber compares the records and determines which match the same person, it merges the contact data to create one contact record.

Dial Plan Mapping

You configure dial plan mapping to ensure that dialing rules on Cisco Unified Communications Manager match dialing rules on your directory.

Application Dial Rules

Application dial rules automatically add or remove digits in phone numbers that users dial. Application dialing rules manipulate numbers that users dial from the client.

For example, you can configure a dial rule that automatically adds the digit 9 to the start of a 7 digit phone number to provide access to outside lines.

Directory Lookup Dial Rules

Directory lookup dial rules transform caller ID numbers into numbers that the client can lookup in the directory. Each directory lookup rule you define specifies which numbers to transform based on the initial digits and the length of the number.

For example, you can create a directory lookup rule that automatically removes the area code and two-digit prefix digits from 10-digit phone numbers. An example of this type of rule is to transform `4089023139` into `23139`.

Cisco Unified Communication Manager UDS for Mobile and Remote Access

Cisco Unified Communication Manager UDS is the contact source used when Cisco Jabber connects using Expressway for Mobile and Remote Access. If you deploy LDAP within the corporate firewall, we recommend that you synchronize your LDAP directory server with Cisco Unified Communications Manager to allow the client to connect with UDS when users are outside the corporate firewall.

Cloud Contact Source

Webex Contact Source

For Cloud deployments, contact data is configured in Webex Messenger Administration Tool or by user updates. The contact information can be imported using the Webex Messenger Administration Tool. For more information see the *User Management* section of the Webex Messenger Administration Guide.

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.